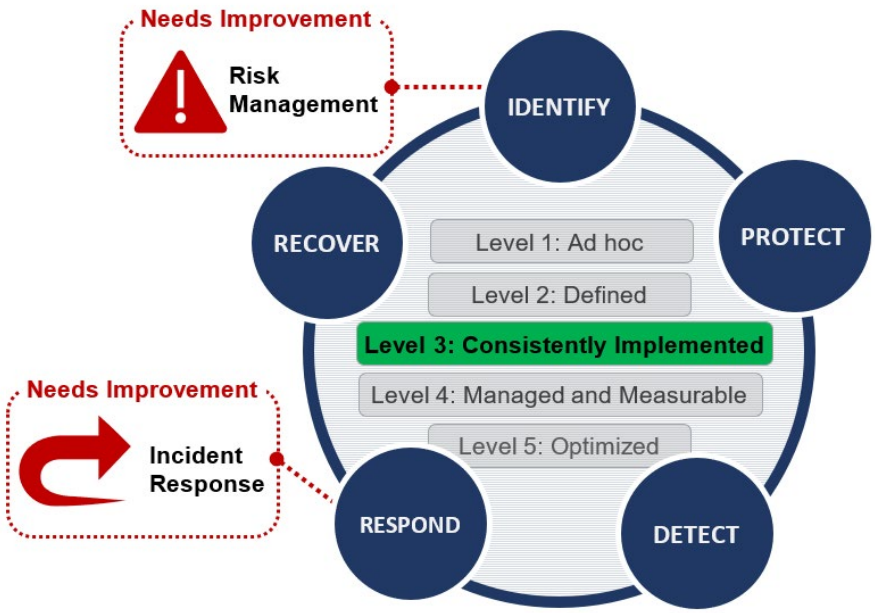
U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

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

# EPA Needs to Improve Its Risk Management and Incident Response Information Security Functions

**Report No. 20-P-0120** **March 24, 2020**



**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 |
| FY | Fiscal Year |
| IG | Inspector General |
| OIG | Office of Inspector General |
| U.S.C. | United States Code |

**Cover Image:** OIG assessment of the EPA's FISMA function areas and domains. (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, D.C. 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, D.C. 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

20-P-0120
March 24, 2020

# At a Glance

**Why We Did This Project**

We performed this audit to assess the U.S. Environmental Protection Agency's compliance with the fiscal year 2019 Inspector General reporting instructions for the Federal Information Security Modernization Act of 2014.

The *FY 2019 IG FISMA Reporting Metrics* outlines five security function areas and eight corresponding domains to help federal agencies manage cybersecurity risks. The document also outlines five maturity levels by which IGs should rate agency information security programs:

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

**This report addresses the following:**

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

**Address inquiries to our public affairs office at (202) 566-2391 or OIG_WEBCOMMENTS@epa.gov.**

**List of OIG reports.**

## *EPA Needs to Improve Its Risk Management and Incident Response Information Security Functions*

### What We Found

**Further implementation of risk management activities and incident response tools are needed to combat cybersecurity threats intended to steal and destroy confidential and sensitive information.**

We assessed the maturity of the EPA's information security program at Level 3, *Consistently Implemented.* A Level 3 designation means that the EPA's policies, procedures, and strategies are consistently implemented but quantitative and qualitative effectiveness measures are lacking. To determine the EPA's maturity level, we reviewed the five security function areas outlined in the *FY 2019 IG FISMA Reporting Metrics:* Identify, Protect, Detect, Respond, and Recover. We also reviewed the eight corresponding domains: Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning.

While the EPA consistently implemented policies, procedures, and strategies for many of these function areas and domains, improvements are still needed:

- **Risk Management**: The EPA did not implement standard data elements for software and associated licenses used within the Agency's information technology environment, and the plans of action and milestones were not consistently used to mitigate security weaknesses.

- **Incident Response:** The EPA did not implement prescribed technologies to support its incident response program.

Appendix A contains the results of our FISMA assessment.

### Recommendations and Planned Agency Corrective Actions

We recommend that the Assistant Administrator for Mission Support (1) develop and maintain an up-to-date inventory of Agency software and associated licenses, (2) establish a control to validate that Agency personnel are creating the required plans of action and milestones associated with vulnerability testing, and (3) implement prescribed technologies to support the EPA's incident response program.

The Agency concurred with our recommendations and provided acceptable corrective actions. All recommendations are considered resolved with planned corrective actions pending.

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

THE INSPECTOR GENERAL

March 24, 2020

**MEMORANDUM**

**SUBJECT:** EPA Needs to Improve Its Risk Management and Incident Response Information Security Functions
Report No. 20-P-0120

**FROM:** Sean W. O'Donnell

**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 of the U.S. Environmental Protection Agency. The project number for this audit was OA&E-FY19-0208. This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. This report represents the opinion of the OIG and does not necessarily represent the final EPA position. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

The Office of Information Security and Privacy within the Office of Mission Support is responsible for the issues discussed in this report.

In accordance with EPA Manual 2750, your office provided acceptable corrective actions in response to the OIG recommendations. All recommendations are resolved, and no final response to this report is required. 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 Act 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.

The report will be available at www.epa.gov/oig.

# Table of Contents



## Appendices

## Purpose

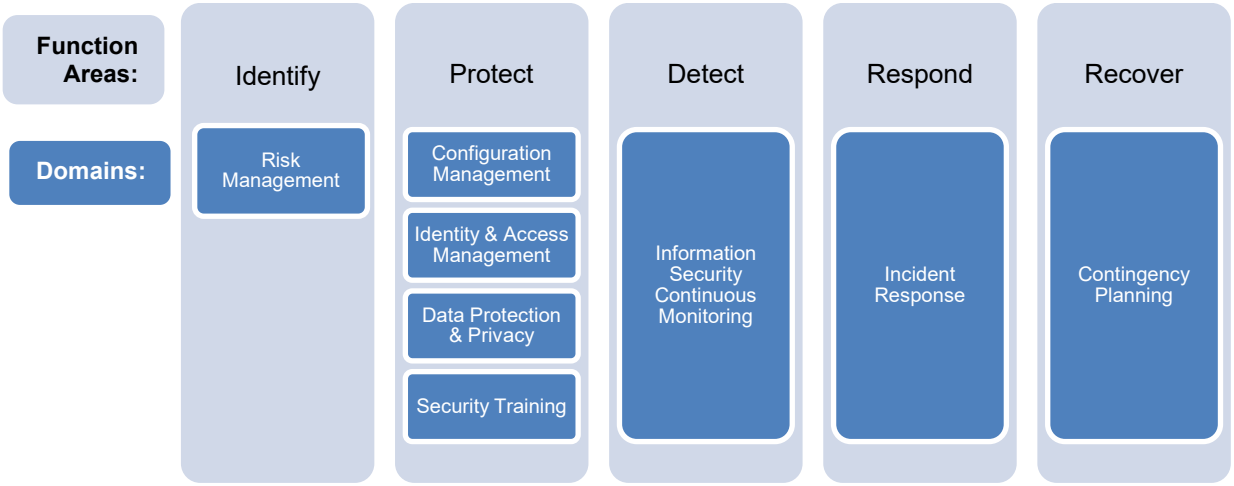
The Office of Inspector General performed this audit to assess the U.S. Environmental Protection Agency's compliance with the fiscal year 2019 Inspector General reporting instructions for the Federal Information Security Modernization Act of 2014.

## Background

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems.[1]

Each fiscal year, the U.S. Department of Homeland Security and the Office of Management and Budget issue an *IG FISMA reporting metric* template for the IG of each federal agency to use to assess the agency's information security program. The *FY 2019 IG FISMA Reporting Metrics,*[2] which can be found in Appendix A, identifies eight domains within five security functions defined in the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Figure 1).[3] This cybersecurity framework provides agencies with a common structure for identifying and managing cybersecurity risks to critical infrastructure across the enterprise.

**Figure 1: FY 2019 cybersecurity framework—five security functions with security domains**



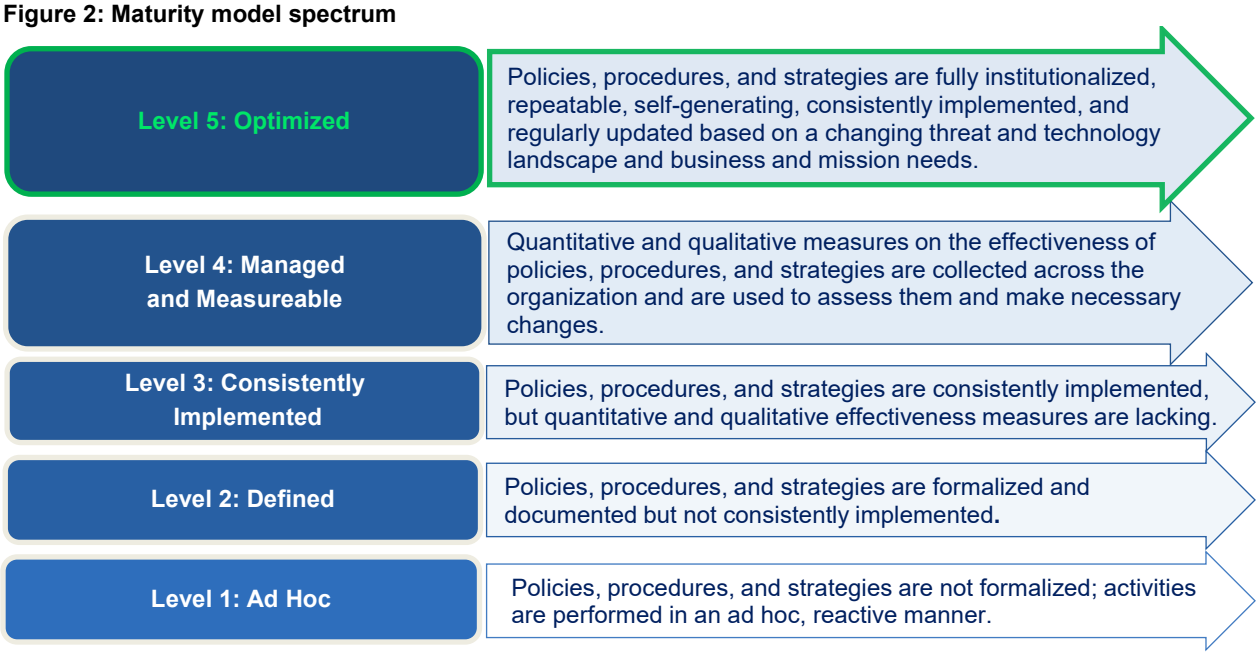

Source: OIG-created graphic based on the *FY 2019 IG FISMA Reporting Metrics* information.

[1] 44 U.S.C. § 3554(a)(1)(A).
[2] *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* Version 1.3, dated April 9, 2019. These metrics were developed as a collaborative effort between the Office of Management and Budget, the U.S. Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency, in consultation with the Federal Chief Information Officer Council.
[3] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, was issued on February 12, 2013, and directed the National Institute of Standards and Technology to develop a voluntary framework based on existing standards, guidelines, and practices to reduce cyber risks to critical infrastructure.

The effectiveness of an agency's information security program is based on a five-tiered maturity model spectrum (Figure 2). An agency's IG is responsible for annually assessing the agency's rating along this spectrum by determining whether the agency possesses the required policies, procedures, and strategies for each of the eight domains. The IG makes this determination by answering a series of questions about the domain-specific criteria that are presented in the annual *IG FISMA Reporting Metrics* template.

An agency must fully satisfy each maturity level before it can be evaluated at the next maturity level. This approach requires the agency to develop the necessary policies, procedures, and strategies for the foundational levels (1 and 2). The advanced levels (3, 4, and 5) describe the extent to which the agencies have institutionalized those policies and procedures.

**Figure 2: Maturity model spectrum**




Source: *FY 2019 IG FISMA Reporting Metrics*.

## Responsible Office

The Office of Mission Support leads the EPA's information management and information technology programs, which provide the necessary information, technology, and services to support the Agency's mission to protect 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 and reports to the Chief Information Officer, is responsible for the EPA's information security program. Additionally, the Chief Information Security Officer is responsible for ensuring that this program complies with FISMA and other information security laws, regulations, directives, policies, and guidelines.

The EPA's 11 program and ten regional offices are responsible for implementing the policies and procedures required by the EPA's information security program. Each program office or region has an information security officer who manages the information security program in that location and monitors compliance with FISMA and related information security directives.

## Scope and Methodology

We conducted this audit from May to December 2019 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 findings and conclusions based on our audit objectives.

We tested whether the EPA implemented the policies and procedures outlined within the *FY 2019 IG FISMA Reporting Metrics* for the FISMA domains within each FISMA security function. We based the level of our testing on the results of a risk assessment of the metrics. The risk assessment considered:

- Key changes in criteria between *FY 2018 IG FISMA Reporting Metrics* and *FY 2019 IG FISMA Reporting Metrics.*
- Metrics rated below Level 3 from the FY 2018 FISMA audit.
- Significant changes to Agency information security policies or procedures.
- Any metrics identified by the EPA OIG or the U.S. Government Accountability Office as an area for improvement in information security during FY 2019.

FISMA reporting metrics that met any of the above considerations were identified as high risk. For these metrics, we conducted our testing through inquiries of Agency personnel, inspections of relevant documentation, and reviews of current EPA OIG audits associated with the metrics outlined in the *FY 2019 IG FISMA Reporting Metrics*. We selected a sample of EPA and contractor systems to evaluate the high-risk FISMA reporting metrics that required testing at the system level. The Office of Mission Support and the Office of Land and Emergency Management have oversight of the sample systems we selected.

Metrics that did not meet any of the above considerations were identified as low risk. For these metrics, we reviewed Agency policies and procedures to determine whether the Agency updated the documents since the OIG's FY 2018 FISMA assessment. We also reviewed the FY 2019 reports issued by the OIG's Office of Audit and Evaluation and the U.S. Government Accountability Office to identify any issues related to the FISMA metrics (Appendix B). If no changes were made

to the EPA's policies and procedures and no other issues were identified for a specific metric, we were able to determine the maturity level for the metric based on our FY 2018 FISMA assessment results.

We worked closely with the EPA and briefed the Agency on the audit results for each function area of the *FY 2019 IG FISMA Reporting Metrics.* Appendix A provides the OIG response to each FISMA metric, as submitted to the Office of Management and Budget on October 18, 2019.

## Results

We concluded that the EPA achieved an overall maturity level of Level 3, which means that the Agency consistently implemented information security policies and procedures but that quantitative and qualitative effectiveness measures are lacking. The OIG assigned a maturity level to each of the eight domains shown in Table 1. These levels are based on a simple majority, where the most frequent maturity level assigned to the metrics within each domain serves as the overall rating for each domain. For example, if a domain has seven metrics and three metrics were rated at Level 2 and four metrics were rated at Level 3, the domain would be rated at Level 3. Similarly, the Agency's overall maturity level is based on a simple majority, where the most frequent maturity level assigned to the individual domains serves as the Agency's overall maturity rating. Table 1 specifies the maturity level we assigned to each function area and the associated domains.

**Table 1: Maturity level of EPA's information security function areas and domains**

| Security function | Security domain | OIG-assessed maturity level |
|---|---|---|
| Identify | Risk Management | Level 3: Consistently Implemented |
| Protect | Configuration Management | Level 3: Consistently Implemented |
| Protect | Identity and Access Management | Level 3: Consistently Implemented |
| Protect | Data Protection and Privacy | Level 3: Consistently Implemented |
| Protect | Security Training | Level 3: Consistently Implemented |
| Detect | Information Security Continuous Monitoring | Level 3: Consistently Implemented |
| Respond | Incident Response | Level 3: Consistently Implemented |
| Recover | Contingency Planning | Level 3: Consistently Implemented |
| EPA's overall maturity rating: Level 3 (Consistently Implemented) | | |

Source: OIG test results.

However, the EPA needs to make improvements within certain individual metrics in the Risk Management and Incident Response domains that were assessed below maturity Level 3, as shown in Table 2.

**Table 2: EPA FISMA metrics that were assessed below maturity Level 3**

| Security function | Security domain | Explanation of metrics areas that need improvement |
|---|---|---|
| Identify | Risk Management | The EPA has not implemented 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 **(Appendix A, metric question 3)**.<br><br>The EPA's plans of action and milestones were not consistently utilized for effectively mitigating security weaknesses **(Appendix A, metric question 8)**. |
| Respond | Incident Response | The EPA has not implemented prescribed technologies to support its incident response program **(Appendix A, metric question 58)**. |

Source: OIG test results.

## Conclusions

While the EPA demonstrated that it had implemented an information security program consistent with the majority of the FISMA metrics, the Agency should continue its efforts to develop a resilient security posture that can prevent, detect, and respond to emerging cyber threats. Improvements in risk management and incident response would allow the Agency to preserve the integrity of EPA data; keep the data available for end users; and protect the data from unauthorized changes, loss, and destruction. Improvements in these areas should also help the Agency increase the maturity level for these critical elements of information security.

## Recommendations

We recommend that the Assistant Administrator for Mission Support:

1. Develop and maintain an up-to-date inventory of the software and associated licenses used within the Agency.

2. Establish a control to validate that Agency personnel are creating the required plans of action and milestones for weaknesses that are identified from vulnerability testing but not remediated within the Agency's established time frames, per the EPA's information security procedures.

3. Implement prescribed technologies to support the EPA's incident response program.

## Agency Response and OIG Assessment

The Office of Mission Support concurred with Recommendation 1, indicated that it addressed a portion of the recommendation, and provided planned corrective actions to address the remaining portion of the recommendation. The EPA stated that it implemented a dashboard and review process that leverages existing capabilities and provides a current inventory of approved software for network endpoints. The EPA provided us with documentation to support that these corrective actions had been implemented. Additionally, the EPA stated that it is developing and deploying an enterprise Software Asset and Configuration Management capability that will align license entitlement data with software inventories to fully realize the goal of this recommendation. The EPA stated that this action would be completed by October 15, 2021. The proposed corrective actions will satisfy the intent of the recommendation, and Recommendation 1 is considered resolved with planned corrective action pending.

The Office of Mission Support concurred with Recommendation 2 and initially indicated that it completed corrective action to address this recommendation. However, we found that the corrective action had not been completed. After additional follow-up with the EPA related to this recommendation, we learned that the corrective action is partially complete, and an Agency representative stated the corrective action would be completed by December 31, 2021. The proposed corrective action satisfies the recommendation, and Recommendation 2 is considered resolved with planned corrective action pending.

The Office of Mission Support concurred with Recommendation 3 and indicated that it has addressed a portion of the recommendation. The Agency also provided planned corrective actions to address the remaining portion of the recommendation. The EPA stated that it implemented a tool that provides integrity controls by continually collecting relevant information for some systems and that the capabilities have been integrated into the Agency's incident response processes. The Agency also stated that it implemented a network-based tool that provides data loss prevention capabilities for cloud related on-premise and cloud services traffic. Additionally, the EPA indicated that it will (1) develop a plan to integrate data loss prevention related capabilities into its incident response processes, (2) identify capability gaps in executing data loss prevention capabilities, and (3) develop gap closing recommendations and related implementation plans by July 31, 2020. The proposed corrective actions satisfy the recommendation, and Recommendation 3 is considered resolved with planned corrective actions pending.

Appendix C includes the Agency's full response to our recommendations.

# *Status of Recommendations and Potential Monetary Benefits*

| RECOMMENDATIONS | | | | | | |
|---|---|---|---|---|---|---|
| **Rec. No.** | **Page No.** | **Subject** | **Status[1]** | **Action Official** | **Planned Completion Date** | **Potential Monetary Benefits (in $000s)** |
| 1 | 5 | Develop and maintain an up-to-date inventory of the software and associated licenses used within the Agency. | R | Assistant Administrator for Mission Support | 10/15/21 | |
| 2 | 5 | Establish a control to validate that Agency personnel are creating the required plans of action and milestones for weaknesses that are identified from vulnerability testing but not remediated within the Agency's established time frames per the EPA's information security procedures. | R | Assistant Administrator for Mission Support | 12/31/21 | |
| 3 | 6 | Implement prescribed technologies to support the EPA's incident response program. | R | Assistant Administrator for Mission Support | 7/31/20 | |

C = Corrective action completed.
R = Recommendation resolved with corrective action pending.
U = Recommendation unresolved with resolution efforts in progress.

**Appendix A**

# *OIG-Completed CyberScope Template*

# Inspector General

Section Report

2019

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. Rev. 4: CA-3, PM-5, and CM8; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2019 CIO FISMA Metrics: 1.1 and 1.4, OMB A-130).

**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 Rev. 4: CA-7 and CM-8; NIST SP 800-137; NISTIR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2019 CIO FISMA Metrics: 1.2 and 3.9.2; CSF: ID.AM-1).

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA Metric 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 Rev. 4: CA7, CM-8, and CM-10; NIST SP 800-137; NISTIR 8011; FEA Framework, v2; FY 2019 CIO FISMA Metrics: 3.10.1; CSF: ID.AM-2)?

**Defined (Level 2)**

**Comments:** The EPA plans to implement technology in fiscal year 2020 to identify authorized and unauthorized software installed on the agency's network.

4 To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets (NIST SP 800-53 Rev. 4: RA-2, PM-7, and PM11; NIST SP 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2019 CIO FISMA Metrics: 1.1; OMB M-19-03)?

**Consistently Implemented (Level 3)**

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

5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy, including for supply chain risk management. This 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 Rev. 4: 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; NIST SP 800-37 (Rev. 2); NIST SP 800-161: Appendix E; CSF: ID.SC-1 – 2; SECURE Technology Act: s. 1326)?

**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; NIST SP 800-160; NIST SP 800-37 (Rev. 2); OMB M-19-03; FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA9, SA-12, and PM-9; NIST SP 800-161; CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

**Consistently Implemented (Level 3)**

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

7 To what degree have roles and responsibilities of internal and external stakeholders involved in risk management processes been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; OMB A-123; CFO Council ERM Playbook; NIST SP 800-37 (Rev. 2); OMB M19-03)?

**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 Rev. 4: CA-5; NIST SP 800-37 (Rev. 2); OMB M-19-03, CSF v1.1, ID.RA-6)?

**Defined (Level 2)**

**Comments:** Based on a sample of critical and high-risk vulnerabilities identified by EPA scans, EPA personnel did not create plans of action and milestones for any of the un-remediated vulnerabilities as required by EPA's information security policy and procedures.

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 800-39; NIST SP 800-53 REV. 4: PL-2 and RA-1; NIST SP 800-30; CSF: Section 4.0; NIST SP 800-37 (Rev. 2))?

**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); OMB M-19-03; CSF: Section 3.3; SECURE Technology Act: s. 1326)?

**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 (NIST SP 800-53 REV. 4: SA-4; NIST SP 800- 152; NIST SP 800-37 Rev. 2; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4).

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 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)?

**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?

**The United States Governmental Auditing Office (GAO) Report GAO-19-384, Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges (issued July 2019), identified improvements in the EPA's risk management program and recommended that the EPA (1) update policies to require an organization-wide cybersecurity risk assessment (2) establish a process to conduct organization-wide cybersecurity risk assessment and (3) establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions. 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

## 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 REV. 4: CM-1; NIST SP 800- 128: Section 2.4)?

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 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 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 REV. 4: 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 REV. 4: 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 REV. 4: CM-2 and CM-8; FY 2019CIO FISMA Metrics: 1.1,2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7and PR.IP-1)?

**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 REV. 4: CM-6, CM-7, and SI-2; FY 2019CIO FISMA Metrics: 1.1 and 2.2; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1and DE.CM-8)?

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 22.

## Function 2A: Protect - Configuration Management

19 To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53 REV. 4: CM-3 and SI-2; NIST SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20,Control 4.5; FY 2019CIO FISMA Metrics: 2.13; CSF: ID.RA-1; DHS Binding Operational Directive(BOD)15-01; DHS BOD 18-02)?

**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.

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 REV. 4: CM-2 and CM-3; CSF: PR.IP-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 REV. 4: AC-1, IA-1, and PS-1; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 32.

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

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 REV. 4: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5)?

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 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 REV. 4: PS-2 and PS-3; National Insider Threat Policy; CSF: PR.IP-11)?

**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 REV. 4: AC-8, PL-4, and PS6)?

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 32.

28 To what extent has the organization implemented strong authentication mechanisms (PIV or a 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 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.4 and 2.7; CSF: PR.AC-1 and 6; 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 (PIV or a 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 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; DHS ED 19-01; and Cybersecurity Sprint)?

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 32.

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

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 2019 CIO FISMA Metrics: 2.3 and 2.5; NIST SP 800-53 REV. 4: AC-1, AC-2 (2), and AC-17; CSIP; DHS ED 19- 01; CSF: PR.AC-4).

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 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 REV. 4: AC-17 and SI-4; CSF: PR.AC-3; and FY 2019 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; NIST SP 800-37 (Rev. 2); OMB M-18- 02; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J)?

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 38.

## Function 2C: Protect - Data Protection and Privacy

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 REV. 4; Appendix J, SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2019 CIO FISMA Metrics: 2.8; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6)?

·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

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 38.

35 To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53 REV. 4: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2019 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?

**Consistently Implemented (Level 3)**

**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 REV. 4: Appendix J, SE-2; FY 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M-17- 25)?

**Consistently Implemented (Level 3)**

**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 REV. 4: 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)

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 38.

## Function 2C: Protect - Data Protection and Privacy

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 3 (Consistently Implemented). Based on our review of the EPA's processes and supporting documentation, we conclude that the EPA has an effective data protection and privacy program.**

**Calculated Maturity Level - Consistently Implemented (Level 3)**

## 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 REV. 4: AT-1; and NIST SP 800-50).

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 45.2.

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 REV. 4: 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 REV. 4: AT-1; NIST SP 800-50: Section 3; CSF: PR.AT- 1).

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 45.2.

## Function 2D: Protect - Security Training

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 REV. 4: 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 REV. 4: AT-2; FY 2019 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4).

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 45.2.

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 REV. 4: AT-3 and AT-4; FY 2019 CIO FISMA Metrics: 2.15)?

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 45.2.

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

**Consistently Implemented (Level 3)**

**Comments:** The Protect Function comprises the following domains: Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training. Overall, we consider the Protect Function effective.

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

## 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 organizationwide approach to ISCM (NIST SP 800-37 (Rev. 2); 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 REV. 4: CA-7, NISTIR 8011) (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.

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 REV. 4: CA-1; NIST SP 800-137; CSF: DE.DP-1; and FY 2019 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 REV. 4: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2); NISTIR 8011; OMB M-14-03; OMB M-19-03)

**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 Function.

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 51.2.

## Function 3: Detect - ISCM

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 REV. 4: 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: 4.2; CSF: RS.RP-1; 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.

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 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2019 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 59.2.

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; CSF: DE.AE-1, PR.DS-6, RS.AN-4, and PR.DS- 8; 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; CSF: RS.MI-1 and 2)

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 59.2.

## Function 4: Respond - Incident Response

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 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 4; 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 (NIST SP 800- 86; NIST SP 800-53 REV. 4: IR- 4; OMB M-18-02; PPD-41).

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 59.2.

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 within its incident response program.

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 REV. 4: 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.

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; CSF: ID.BE-5, PR.IP-9, and ID.SC-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 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17- 09; FY 2019 CIO FISMA Metrics: 5.1; CSF:ID.RA-4)?

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 67.2.

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 REV. 4: CP-2; NIST SP 800- 34; FY 2019 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?

**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 REV. 4: CP-3 and CP-4; FY 2019 CIO FISMA Metrics: 5.1; CSF: ID.SC-5 and CSF: PR.IP-10)?

**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 REV. 4: 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 2019 CIO FISMA Metrics: 5.1.1; and NARA guidance on information systems security records)?

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 67.2.

## Function 5: Recover - Contingency Planning

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 REV. 4: CP-2 and IR-4)?

**Consistently Implemented (Level 3)**

**Comments:** See comment in FISMA metric 67.2.

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)**

## Function 0: Overall

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

**Effective**

**Comments:** Overall, the EPA's information security program is considered effective at maturity level 3 (Consistently Implemented)

## 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.

·Do not include the names of specific independent auditors, these entities should be referred to as "independent assessor" or "independent auditor"

·The assessment of effectiveness should not include a list of ratings by NIST CSF Function-level, as these will already be included in the performance summary

**The EPA has an effective information security program for the following eight security functions and related domains defined within the FY 2019 Inspector General (IG) Federal Information Security Modernization Act (FISMA) Reporting Metrics:**

- **Risk Management**
- **Configuration Management**
- **Identity and Access Management**
- **Data Protection and Privacy**
- **Security Training**
- **Information Security Continuous Monitoring**
- **Incident Response**
- **Contingency Planning**

**Overall, 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 FY 2019 Inspector General Federal Information Security Modernization Act reporting metrics.**

## APPENDIX A: Maturity Model Scoring

### Function 1: Identify - Risk Management

| Function | Count |
|---|---|
| Ad-Hoc | 0 |
| Defined | 2 |
| Consistently Implemented | 10 |
| Managed and Measurable | 0 |
| Optimized | 0 |
| **Function Rating: Consistently Implemented (Level 3)Not Effective** | |

### 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** | |

### 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** | |

### Function 2C: Protect - Data Protection and Privacy

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

### Function 2D: Protect - Security Training

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

### 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** | |

### Function 4: Respond - Incident Response

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

### Function 5: Recover - Contingency Planning

| Function | Count |
|---|---|
| Ad-Hoc | 0 |
| Defined | 0 |
| Consistently Implemented | 7 |
| Managed and Measurable | 0 |
| Optimized | 0 |
| **Function Rating: Consistently Implemented (Level 3)Not Effective** | |

### 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) | The Protect Function comprises the following domains: Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training. Overall, we consider the Protect Function effective. |
| 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 | Overall, the EPA's information security program is considered effective at maturity level 3 (Consistently Implemented) |

**Appendix B**

# *Information Security Reports Issued in FY 2019*

The EPA OIG issued the following reports in FY 2019 that included recommendations regarding improvements within the EPA's information security program:

- **Report No.** 19-P-0283, *Follow-Up Audit: EPA Took Steps to Improve Records Management* (issued August 27, 2019): The EPA completed all corrective actions for 13 past audit recommendations related to its records management and Freedom of Information Act practices. While the EPA completed corrective actions on all the past recommendations, the Freedom of Information Act statute changed in 2016, and the EPA updated its Freedom of Information Act regulations in June 2019. Consequently, the EPA's Freedom of Information Act policy and procedure again require management review to determine whether updates are needed.

- **Report No.** 19-P-0278, *EPA Oversight over Enterprise Customer Service Solution Needs Improvement* (issued August 19, 2019): The EPA did not implement key oversight activities for the Enterprise Customer Service Solution to meet several Agency software requirements. These activities included documenting the Agency's business justification, having the required plans, and doing a user satisfaction review. Further, the Enterprise Customer Service Solution was not classified into the correct information technology investment category. Office of Management and Budget memorandums describe the Agency's management oversight responsibilities for information systems. The EPA System Life Cycle Management policy and procedures provide a framework for system and project managers to tailor system life cycle management controls for information systems. The EPA Capital Planning and Investment Control policy and procedures identify the classification requirements for information technology investments. The problems we identified existed because the Enterprise Customer Service Solution team did not have processes in place to transfer ownership during the responsible office's reorganization in 2016, document delivery of the vendor's annual deliverables, and verify cloud service vendor compliance with mandatory federal information technology security requirements. In addition, the Enterprise Customer Service Solution team did not identify and report that annual costs exceeded a $250,000 threshold, which would have placed the project into a different information technology investment category with additional reporting requirements. This occurred because the Capital Planning and Investment Control team lacked a process to validate the costs for information technology investments, and the team did not complete the corrective action for a prior 2015 OIG audit recommendation.

- **Report No.** 19-P 0195, *Pesticide Registration Fee, Vulnerability Mitigation and Database Security Controls for EPA's FIFRA and PRIA Systems Need Improvement* (issued June 21, 2019): The EPA has adequate controls over the posting of Federal Insecticide, Fungicide, and Rodenticide Act and Pesticide Registration Improvement Act

financial transactions into the Agency's accounting system (Compass Financials). However, the EPA's systems have internal control deficiencies relating to the fee registration process, system vulnerability mitigation, and database security. We tested controls in these areas to verify their compliance with federal standards and guidance, as well as with EPA policies and procedures. There were inconsistencies and errors related to transactions in the areas of Federal Insecticide, Fungicide, and Rodenticide Act and Pesticide Registration Improvement Act fee data posted between the Office of Pesticide Programs' pesticide registration system and Compass Financials. Out of the 29 high-level vulnerabilities identified by the Agency in 2015 and 2016, 20 remained uncorrected after the allotted remediation time frame. In addition, we tested 10 of the 20 uncorrected vulnerabilities and found that required plans of action and milestones for remediation were not created for any of them. The Office of Pesticide Programs needs to improve the security for one of the Federal Insecticide, Fungicide, and Rodenticide Act and Pesticide Registration Improvement Act databases, including password controls, timely installation of security updates, and restriction of administrative privileges.

- **Report No.** 19-P-0158, *Insufficient Practices for Managing Known Security Weaknesses and System Settings Weaken EPA's Ability to Combat Cyber Threats* (issued May 21, 2019): EPA personnel did not manage plans of action and milestones for remediating security weaknesses within the Agency's information security weakness tracking system as required by EPA policy. This happened because the office responsible for identifying vulnerabilities relies on other Agency offices to enter the plans of action and milestones in the tracking system to manage vulnerabilities that are not remediated. We identified one EPA office that was tracking vulnerabilities outside the tracking system, while another office indicated that it did not have a formal process to create plans of action and milestones in the system. Without accessible and consistent information about weaknesses that are not remediated, senior EPA managers cannot make risk-based decisions on how to protect the Agency's network against cybersecurity threats. Additionally, the EPA's information security weakness tracking system lacked controls to prevent unauthorized changes to key data fields and to record these changes in the system's audit logs. This occurred because the EPA neither enabled the feature within the tracking system to prevent unauthorized modifications to key data nor configured the system's logging feature to capture information on the modification of key data fields. As a result, unauthorized changes to the system's data could occur and hamper the Agency's ability to remediate existing system weaknesses.

- **Report No.** 19-N-0085, *Management Alert – Destruction of a Document Used to Certify Security of EPA's Budget Formulation System* (issued March 8, 2019): While conducting the audit of information system security controls for the EPA's budget systems, the OIG requested the *Budget Formulation System Security Assessment Report* for the cloud-hosting environment and the Office of the Chief Financial Officer's analysis of the report. The Office of the Chief Financial Officer personnel said that a nondisclosure agreement with the U.S. General Services Administration's Federal Risk and Authorization Management Program prohibited the EPA from sharing the Agency's review of third parties. The Office of the Chief Financial Officer personnel said that, because of the nondisclosure agreement they had signed, they destroyed the notes documenting their

analysis of the security assessment report. When an Office of the Chief Financial Officer employee made notes of the Office's review of the Budget Formulation System controls—and the employee was aware of the audit because the OIG had issued an audit notification memorandum on December 17, 2017—it put the document squarely in the realm of information subject to disclosure in the course of the OIG audit. The proper course of action for the Office of the Chief Financial Officer would have been to (1) not destroy the notes, (2) notify the OIG audit team of the issue with the notes and the nondisclosure agreement, and (3) provide the notes to the audit team as required by Section 6(a)(1) of the Inspector General Act of 1978, as amended, 5 U.S.C. app.

**Appendix C**

# *Agency Response to Draft Report*

**MEMORANDUM**

**SUBJECT:** Response to Office of Inspector General Draft Report No. OA&E-FY19-0208 "EPA Needs to Improve Its Risk Management and Incident Response Information Security Functions" dated December 16, 2019

**FROM:** Vaughn Noga, Chief Information Officer and Deputy Assistant Administrator for Environmental Information

VAUGHN NOGA Digitally signed by VAUGHN NOGA Date: 2020.01.23 13:34:16 -05'00'

**TO:** Rudolph M. Brevard, Director
Information Resources Management Directorate
Office of Audit and Evaluation

Thank you for the opportunity to respond to the issues and recommendations in the subject audit report. Following is a summary of the Office of Mission Support's (OMS) overall position, along with its position on each of the report recommendations. We have already addressed recommendations 2 and 3, as outlined below. We propose a corrective action to complete recommendation 1.

AGENCY'S RESPONSE TO REPORT RECOMMENDATIONS

Agreements

| No. | Recommendation | High-Level Intended Corrective Action (s) | Estimated Completion Date |
|---|---|---|---|
| 1 | Develop and maintain an up-to-date inventory of the software and associated licenses used within the organization | The agency implemented a dashboard and review process that leverages existing capabilities and provides a current inventory of approved software for network endpoints. | Completed Asset Inventory |
| | | Establishing License Entitlement Inventory. The agency is developing and deploying an enterprise Software Asset and Configuration Management (SACM) capability that will align license entitlement data with software inventories to fully realize the goal of this recommendation. | October 15, 2021 |

| No. | Recommendation | High-Level Intended Corrective Action (s) | Estimated Completion Date |
|---|---|---|---|
| 2 | Establish a control to validate that agency personnel are creating the required plans of action and milestones for weaknesses identified from vulnerability testing but not remediated within the agency's established timeframes per the EPA's information security procedures. | The agency has a documented plan of actions and milestones for a monitoring, validation and verification process. The process is used for all sources of vulnerabilities to include those from vulnerability scanning. | Completed |
| 3 | Implement file integrity and data loss prevention tools to support the EPA's incident response program. | The agency implemented a host-based tool, Defender Advanced Threat Protection, that provides integrity controls by continually collecting relevant information to include information on registry and file system changes for Microsoft based systems. The capabilities have been integrated into the agency's incident response processes.<br><br>The agency implemented a network-based tool, Microsoft Cloud App Security, that provides data loss prevention capabilities for cloud related on-premise and cloud services traffic. The tool provides indications of possible unauthorized data movement on the network and in the cloud.<br><br>The agency will:<br>develop a playbook to integrate MCAS DLP related capabilities into incident response processes;<br><br>identify capability gaps - tools, processes, people - in executing DLP capabilities; | Completed<br><br>February 28, 2020 |

| No. | Recommendation | High-Level Intended Corrective Action (s) | Estimated Completion Date |
|---|---|---|---|
| | | develop gap closing recommendations;<br><br>identify which gap closing recommendations can be implemented in FY2021 and develop implementation plans; | <br><br>July 31, 2020 |

If you have any questions regarding this response, please contact Mitchell Hauser, OMS' Audit Follow-up Coordinator, on (202) 564-7636.

cc: Vincent Campbell
Nancy Dao
Eric Jackson, Jr.
Gina Ross
Scott Sammons
Erin Collard
Robert McKinney
Jeffery Anouilh
Lee Kelly
Brian Epley
David Updike
Lynnann Hitchens
Daniel Coogan
Janice Jablonski
Marilyn Armstrong
Mitchell Hauser
David Zeckman
Annette Morant
Andrew LeBlanc

# *Distribution*

The Administrator
Assistant Deputy Administrator
Associate Deputy Administrator
Chief of Staff
Deputy Chief of Staff/Operations
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
Associate Deputy Assistant Administrator for Mission Support
Deputy Assistant Administrator for Environmental Information and Chief Information Officer, Office of Mission Support
Director, Information Security and Management Staff, Office of Mission Support
Senior 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