



OFFICE OF INSPECTOR GENERAL

U.S. ENVIRONMENTAL PROTECTION AGENCY

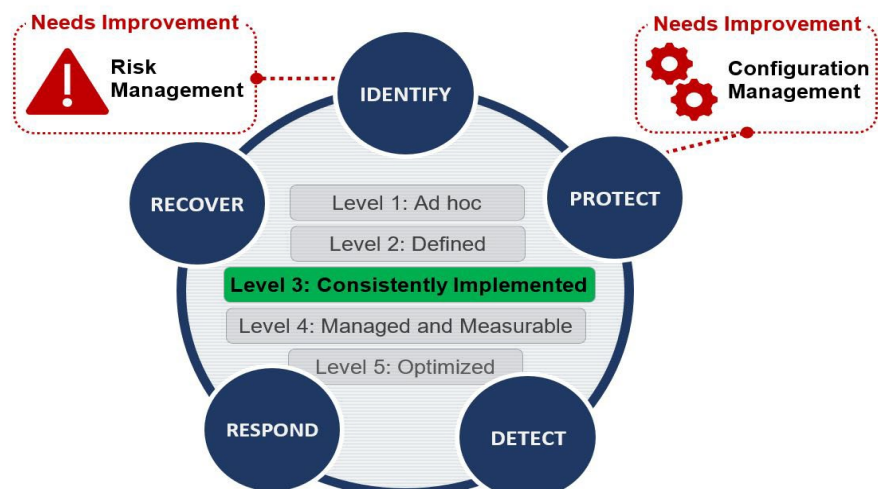
CUSTOMER SERVICE ★ INTEGRITY ★ ACCOUNTABILITY

*Compliance with the law
Operating effectively and efficiently*

The EPA Lacks Documented Procedures for Detecting and Removing Unapproved Software on the Agency's Network

Report No. 22-E-0028

March 30, 2022



Report Contributors: LaSharn Barnes
LaVonda Harris-Claggett
Eric Jackson Jr.
Alonzo Munyeneh
Jeremy Sigel
Sabrena Stewart

Abbreviations:	CIO	Chief Information Officer
	EPA	U.S. Environmental Protection Agency
	FISMA	Federal Information Security Modernization Act of 2014
	FY	Fiscal Year
	IG	Inspector General
	IT	Information Technology
	OIG	Office of Inspector General
	U.S.C.	United States Code

Key Definitions: *Please see Appendix A for key definitions.*

Cover Image: The EPA has consistently implemented its information security policies and procedures, but quantitative and qualitative effectiveness measures are lacking. (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, 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](#).



Office of Inspector General U.S. Environmental Protection Agency **At a Glance**

22-E-0028
March 30, 2022

Why We Did This Evaluation

We performed this evaluation to assess the U.S. Environmental Protection Agency's compliance with the *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* and determine whether the EPA followed its processes to investigate and remove unapproved software from the network.

The reporting metrics outline five security function areas and nine corresponding domains to help federal agencies manage cybersecurity risks. The document also outlines five maturity levels by which inspectors general should rate their agencies' information security programs:

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

This evaluation supports EPA mission-related efforts:

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

This evaluation addresses a top EPA [management challenge](#):

- *Protecting information technology and systems against cyberthreats.*

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

[List of OIG reports.](#)

The EPA Lacks Documented Procedures for Detecting and Removing Unapproved Software on the Agency's Network

What We Found

We concluded that the EPA achieved an overall maturity level of Level 3 (Consistently Implemented) for the five security functions and nine domains outlined in the *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*. This means that the EPA consistently implemented its information security policies and procedures, but quantitative and qualitative effectiveness measures are lacking. We

identified that the EPA has deficiencies in documenting software management procedures on the detection and removal of nonbase software, which is software that is not part of the standard Agency package.

Without documented procedures governing software management and vulnerability remediation processes, the EPA continues to be at risk of outsiders gaining access to compromise and exploit Agency systems and data.

Recommendations and Planned Agency Corrective Actions

We recommend that the Office of Mission Support document procedures to detect and remove unapproved software on the Agency's network and provide targeted training on those procedures. The Agency agreed and provided acceptable planned corrective actions with estimated completion dates to address the recommendations.

Noteworthy Achievement

The Agency developed a software triage team in response to an August 2019 chief information officer memorandum to senior information officers asking them to certify software on the EPA network. The software triage team maintains an agencywide dashboard available to all information management officers that shows all software loaded on program office and regional computers. The team meets regularly to discuss the justification for unapproved software discovered on the network or the information management officers' plans for software removal and updates the dashboard accordingly.




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

THE INSPECTOR GENERAL

March 30, 2022

MEMORANDUM

SUBJECT: The EPA Lacks Documented Procedures for Detecting and Removing Unapproved Software on the Agency's Network
Report No. 22-E-0028

FROM: Sean W. O'Donnell 

TO: Kimberly Patrick, Principal Deputy Assistant Administrator
Office of Mission Support

This is our report on the subject evaluation conducted by the Office of Inspector General of the U.S. Environmental Protection Agency. The project number for this evaluation was [OA-FY21-0206](#). This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

The Office of Mission Support is responsible for the issues discussed in this report.

In accordance with EPA Manual 2750, your office provided acceptable planned corrective actions and estimated milestone dates in response to OIG recommendations. All recommendations are resolved, and no final response to this report is required. If you submit a response, however, 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.

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

Table of Contents

Chapters

1	Introduction	1
	Purpose.....	1
	Background.....	1
	Responsible Offices	3
	Noteworthy Achievement	4
	Scope and Methodology.....	4
	Prior Report	5
	Results	6
2	Documented Procedures and Targeted Training Needed on Detection and Removal of Unapproved Software	7
	EPA Lacks Documented, Formalized Processes to Address Unapproved Software on Its Network.....	7
	Recommendations.....	8
	Agency Response and OIG Assessment.....	8
	Status of Recommendations.....	10

Appendixes

A	Key Definitions	11
B	OIG-Completed CyberScope Template	12
C	Information Security Reports Issued in FY 2021	34
D	EPA FY 2021 FISMA Compliance Results	36
E	Agency Response to Draft Report	37
F	Distribution	40

Chapter 1

Introduction

Purpose

The U.S. Environmental Protection Agency's Office of Inspector General [initiated](#) this evaluation to (1) assess the EPA's compliance with the fiscal year 2021 inspector general reporting instructions for the Federal Information Security Modernization Act of 2014 and (2) determine whether the EPA followed its processes to investigate and remove unapproved software from the network.

Top Management Challenge

This evaluation addresses a top management challenge for the Agency, as identified in OIG Report No. [22-N-0004](#), *EPA's Fiscal Year 2022 Top Management Challenges*, issued November 12, 2021:

- Protecting information technology and systems against cyberthreats.

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 collected, maintained, or used by or on behalf of the agency.¹

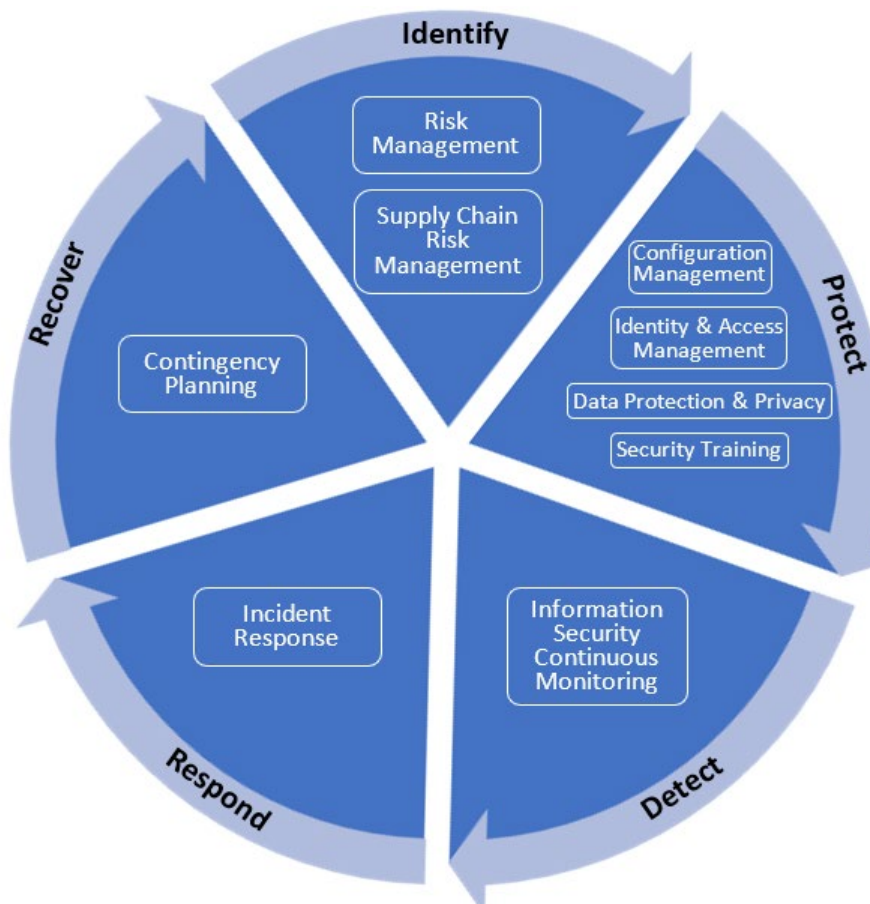
Each fiscal year, the U.S. Department of Homeland Security and the Office of Management and Budget issue the FISMA reporting metrics template to the IG of each federal agency to assess the agency's information security program. These metrics were developed as a collaborative effort among the Office of Management and Budget, the Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency, in consultation with the Federal Chief Information Officer Council. The *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, dated May 12, 2021, identified nine domains within five security function areas defined in the National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, dated April 16, 2018 (Figure 1).² The document contains 66 metrics for IGs to assess. These metrics and their assessed ratings are in Appendix B.

This cybersecurity framework provides agencies with a common structure for identifying and managing cybersecurity risks to critical infrastructure across the enterprise.

¹ 44 U.S.C. § 3554(a)(1)(A).

² 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 cybersecurity framework based on existing industry standards, guidelines, and practices to reduce cyberrisks to critical infrastructure.

Figure 1: FY 2021 cybersecurity framework—five security functions with nine security domains



Source: OIG summary of the *FY 2021 IG FISMA Reporting Metrics*. (EPA OIG image)

The effectiveness of an agency's information security program is based on a five-tiered maturity model spectrum (Figure 2). Each 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 nine 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.

Figure 2: Maturity model spectrum



Source: *FY 2021 IG FISMA Reporting Metrics*. (EPA OIG image)

Within the maturity model spectrum, the agency should perform risk assessments and identify the optimal maturity level that achieves cost-effective security when considering the agency's missions and risks. This approach requires the agency to develop the necessary policies, procedures, and strategies to meet effective levels of security, including the more advanced maturity levels (3, 4, and 5) for which the agency has consistently and effectively implemented and institutionalized those policies and procedures.

Additionally, in January 2021, we received a hotline complaint alleging there was unapproved software on the EPA's network. Unapproved software exposes the Agency's network to the risk of a cybersecurity breach if unauthorized users gain access to the network through such software to exploit its systems and data. The Ponemon Institute's *Cost of a Data Breach Report 2021* puts the average cost of a data breach in the United States at \$9.05 million, with an average public sector cost of \$1.93 million per data breach. As part of our assessment of the Risk Management FISMA domain, we reviewed the Agency's processes for detecting and removing software on the network.

Responsible Offices

The Office of Mission Support leads the EPA's information management and information technology programs. It is responsible for providing the necessary information, technology, and services to support the Agency's mission. Within the Office of Mission Support, the:

- Chief information security officer is responsible for the EPA's information security program and ensures that the program complies with FISMA and other information security laws, regulations, directives, policies, and guidelines.

- Office of Information Technology Operations is responsible for providing procedures, standards, and training on the Agency's software management policy and documentation, confirmation, and approval of individuals using IT resources across the Agency.
- Office of Information Security and Privacy promotes agencywide cooperation in managing risks and protecting EPA information and defines clear, comprehensive, and enterprisewide information security and privacy strategies.

Noteworthy Achievement

The Agency developed a software triage team in response to an August 2019 chief information officer, or CIO, memorandum to senior information officers asking them to certify software on the EPA network. The software triage team maintains an agencywide dashboard available to all senior information officers and information management officers that shows all software loaded on program office and regional computers. The team meets regularly to discuss justification for unapproved software discovered on the network or the information management officers' plans for software removal.

Scope and Methodology

We conducted this evaluation from June to December 2021 in accordance with the *Quality Standards for Inspection and Evaluation* published in January 2012 by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings, conclusions, and recommendations based on our objectives. We believe that the evidence obtained provides a reasonable basis for our findings, conclusions, and recommendations based on our review.

We assessed whether the EPA achieved Maturity Level 3 (Consistently Implemented) for the FISMA domains within each FISMA security function area, which denotes that its policies, procedures, and strategies consistently adhere to the *FY 2021 IG FISMA Reporting Metrics*. However, for the Supply Chain Risk Management domain, which was added in FY 2021, we only assessed whether the Agency had defined procedures, in adherence with Maturity Level 2 (Defined), because of the *FY 2021 IG FISMA Reporting Metrics'* guidance that agencies be given one calendar year from the requirements' publication to fully implement its underlying criteria.

We reviewed the information security reports that we issued in FY 2021 (Appendix C) and reports issued by the U.S. Government Accountability Office to identify weaknesses within the EPA's information security program related to the FY 2021 FISMA metrics. We reviewed EPA policies and procedures to identify significant changes made to the Agency's governance practices that would affect the Agency's ability to meet the FY 2021 FISMA metrics. We used this information and compared the FY 2020 and FY 2021 FISMA reporting metrics within our risk assessment to determine our level of testing for this evaluation. We defined a metric as high risk if it met one of the following criteria:

- Our FY 2020 assessment rating of the metric would materially change because of a key change between the FY 2020 and FY 2021 IG FISMA reporting metrics' underlying criteria.
- Our rating of the metric was below Level 3 in our FY 2020 FISMA evaluation.

- Our FY 2020 assessment for the metric would materially change because of significant changes to the EPA's information security policies or procedures.

For these high-risk metrics, we spoke with Agency personnel, inspected relevant Agency IT documentation, and analyzed evidence supporting EPA compliance with the metrics outlined in the *FY 2021 IG FISMA Reporting Metrics*. We rated the metrics as low risk if they did not meet any of the above criteria. Additionally, 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 2020 FISMA assessment results.

Based on the *FY 2021 IG FISMA Reporting Metrics* reporting instructions, the overall maturity level for each domain is calculated based on a simple majority. In other words, the most frequent maturity level assigned to the individual domains serves as the agency's overall maturity rating. For example, if a domain has seven metrics questions and three metrics questions were rated at Level 2 and four metrics questions were rated at Level 3, the domain would be rated at Level 3. This calculation is performed automatically by the Office of Management and Budget's CyberScope system, which the IGs use to report their assessment results. Although IGs have flexibility in determining the overall rating, the *FY 2021 IG FISMA Reporting Metrics* recommend that the agency's overall maturity level be based on a simple majority.

We followed up on the hotline complaint via the Risk Management domain metrics to determine whether the EPA followed its processes to investigate and remove nonbase software, which is software that is not part of the standard Agency package, on the EPA network. Our follow-up consisted of:

- Interviewing all parties mentioned in the hotline complaint and obtaining documentation to verify their statements about the Agency's software management processes.
- Analyzing the June 2021 report from the EPA Computer and Software regarding nonbase software installed on Agency computers and selecting ten high-risk instances to review.
- Interviewing the information management officers responsible for managing software for the five regional and program office networks in which ten instances of high-risk software were discovered. We gained an understanding of their processes, reviewed the guidance provided by headquarters, and documented the procedures relating to the detection and removal process.
- Requesting documentation supporting approval of the ten high-risk software instances.
- Obtaining listings of privileged users who have the ability to install software on the five region and program office networks to verify whether the listings are reviewed on a regular basis.

We provided our assessment of each function area of the *FY 2021 IG FISMA Reporting Metrics* and discussed the results with the Agency. Appendix D provides the OIG's assessment for each FISMA metrics, as submitted to the Office of Management and Budget on October 29, 2021.

Prior Report

We followed up on the five recommendations made in OIG Report No. [21-E-0124](#), *EPA Needs to Improve Processes for Updating Guidance, Monitoring Corrective Actions, and Managing Remote Access for External Users*, issued April 16, 2021. These recommendations addressed weaknesses found in our

FY 2020 FISMA audit, which included verifying that corrective actions were completed before closing the audit report's recommendations in the EPA audit tracking system and designating a governance structure for the Agency's identity, credential, and access management process. We reported that the EPA provided acceptable corrective actions to address our five recommendations. When the report was issued, two of the recommendations were completed and the remaining were considered resolved with planned corrective actions pending.

Results

We concluded that the EPA achieved an overall maturity level of Level 3 (Consistently Implemented) for the five security functions and nine domains outlined in the *FY 2021 IG FISMA Reporting Metrics* (Appendix D). This conclusion means that the EPA consistently implemented its information security policies and procedures, but quantitative and qualitative effectiveness measures are lacking. We found the EPA has the following deficiencies: its software management process lacks documented procedures and targeted training for detecting and removing unapproved software installed on its region and program office networks.

See Chapter 2 for a detailed analysis of the above findings.

Chapter 2

Documented Procedures and Targeted Training Needed on Detection and Removal of Unapproved Software

Our evaluation of a hotline complaint determined that while processes were in place to investigate and remove unapproved software, these processes were ad hoc and the Agency lacked documented procedures and targeted training for detecting and removing unapproved software. This resulted in software being installed on the EPA's regional and program office network without documented authorization. Federal, as well as Agency, guidance requires authorization for acquiring and using computer software on the EPA's network. Unauthorized software puts the Agency's network, including systems and data, at risk of being compromised from exploited vulnerabilities associated with unapproved software on EPA network.

EPA Lacks Documented, Formalized Processes to Address Unapproved Software on Its Network

A June 2021 report from the EPA Computer and Software Dashboard provided by the Agency's software triage team identified over 7,000 instances of nonbase software on its network. The report listed foreign software and malware programs that gather user information, allow remote control and viewing of the EPA user's computer via virtual network computing, and have a history of targeted attacks. Focusing on these types of instances, we selected ten instances of software installed on the networks of one program office and four regional offices. Our analysis found that all ten of the software instances (100 percent) were unapproved (Figure 3).

Figure 3: Ten of the software instances reviewed (100 percent) were unapproved



Source: OIG analysis of installed software. (EPA OIG image)

Based on interviews conducted with ten IT personnel responsible for managing the software that we reviewed (Table 1), as well as members of the software triage team, the chief information security officer, the deputy director of the Office of Information and Technology Operations, and the CIO, we determined that the Agency lacks documented software management procedures and targeted training for detecting and removing unapproved software on EPA network. In addition, their responses revealed that the software management program lacks processes related to established time frames for removal

of unapproved software, risk classifications, and formal identification of software that collects privacy data.

Table 1: EPA IT personnel responses on software management deficiencies

Software management deficiencies identified	IT personnel affirmative responses									
	1	2	3	4	5	6	7	8	9	10
No established time frames for removing unapproved software.	X			X	X			X	X	X
No established risk classifications for unapproved software.									X	
No formal process to identify and prioritize removing software that collects privacy data.									X	X
No documented process for detecting and removing unapproved software.			X	X	X				X	X
No targeted software management training.	X		X		X	X				X

Source: OIG analysis of EPA IT personnel interview responses. (EPA OIG table)

Executive Order 13103, *Computer Software Piracy*, dated September 30, 1998, requires agency heads to “ensure that only authorized computer software is acquired for and used on the agency’s computers.” Additionally, CIO 2104-P-01.1, *Software Management and Piracy Procedure*, dated August 29, 2019, requires each program office and region to only install software that is approved for use on EPA computer systems, to approve software for use within their office, and to monitor all systems to ensure that no unauthorized software is uploaded.

Without documented procedures governing the software management process—specifically procedures for detecting and removing unapproved software—the Agency continues to be at risk from unauthorized software that is installed on its network. While the Agency has worked to reduce the number of unapproved software instances on EPA network, the presence of over 7,000 instances of nonbase software on the Agency’s network, according to a June 2021 dashboard report, demonstrates the risk of outsiders gaining access to Agency systems and data to compromise and exploit them.

Recommendations

We recommend that the assistant administrator for Mission Support:

1. Develop and document procedures for detecting and removing unapproved software on the Agency’s network, to include time frames for removal, risk classifications, and identification of software collecting privacy data.
2. Develop and provide training on the Agency’s processes for detecting and removing unapproved software to users with privileges to install software on the EPA’s network.

Agency Response and OIG Assessment

The EPA concurred with our two recommendations and provided acceptable planned corrective actions and estimated milestone dates for these recommendations.

The Office of Mission Support concurred with Recommendation 1 and recognized that the Agency's software management procedures can be updated to clearly outline the current processes for software certification, as well as the identification and removal of unapproved software from EPA's network, and will complete the update accordingly. We believe that the proposed corrective action will satisfy the intent of the recommendation. Therefore, we consider Recommendation 1 resolved with corrective action pending.

The Office of Mission Support concurred with Recommendation 2 and indicated that it would provide training on the process for detecting and removing unapproved software. We believe that this corrective action meets the intent of the recommendation and therefore consider Recommendation 2 resolved with corrective action pending.

The draft report recommended that the Agency update its information security procedures to comply with Department of Homeland Security requirements for remediation of critical vulnerabilities. Following discussions with the Agency, we determined that this does not require a corrective action plan due to the Agency procedures being more stringent than the Department of Homeland Security directive. Therefore, we removed this recommendation.

Status of Recommendations

RECOMMENDATIONS

Rec. No.	Page No.	Subject	Status ¹	Action Official	Planned Completion Date
1	8	Develop and document procedures for detecting and removing unapproved software on the Agency's network, to include time frames for removal, risk classifications, and identification of software collecting privacy data.	R	Assistant Administrator for Mission Support	10/31/22
2	8	Develop and provide training on the Agency's processes for detecting and removing unapproved software to users with privileges to install software on the EPA's network.	R	Assistant Administrator for Mission Support	1/31/23

¹ C = Corrective action completed.

R = Recommendation resolved with corrective action pending.

U = Recommendation unresolved with resolution efforts in progress.

Key Definitions

Domains: Function areas are broken down into nine domains developed to promote consistent and comparable metrics and criteria when assessing the effectiveness of the agencies' information security programs.

Function area: Five function areas make up the cybersecurity framework that provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and IGs with guidance for assessing the maturity of controls to address those risks.

Metrics: FISMA reporting guidance consists of 66 metrics, which are questions divided among nine domains to provide reporting requirements across key areas to be addressed in the independent evaluations of agencies' information security programs.

Nonbase software: Software that is not part of the Agency's standard installation or otherwise loaded onto workstations as part of regular business.

Software: Programs and applications that run on a computer, such as word processors, spreadsheets, and databases.

Underlying criteria: The 66 metrics were developed from underlying criteria consisting of Office of Management and Budget, Department of Homeland Security, Council of the Inspectors General on Integrity and Efficiency, and Federal CIO Council guidance and security control requirements relevant to that metric's cybersecurity risk.

OIG-Completed CyberScope Template



Environmental Protection Agency

Function 0: Overall

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

Effective

Comments: See remarks in question 0.2.

- 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.

EPA has demonstrated it has consistently implemented policy, procedures, and strategies for all five of its information security function areas. The Office of Inspector General assessed the five Cybersecurity Framework function areas and concluded that EPA has achieved a Level 3, Consistently Implemented, which denotes that the Agency has consistently implemented policies, procedures, and strategies in adherence to the Fiscal Year 2021 Inspector General Federal Information Security Modernization Act reporting metrics. While EPA has policies, procedures, and strategies for these function areas and domains, improvements are still needed in the following areas: (1) Risk Management - EPA's software management process lacks documented procedures for detecting and removing unapproved software on the EPA network resulting in unapproved software installed on its region and program office networks. (2) Configuration Management - EPA has not updated its Risk Assessment or Systems and Information Integrity procedures to meet the Department of Homeland Security Binding Operational Directive 19-12, Vulnerability Remediation Requirements for Internet-Accessible Systems, a federal requirement for remediating critical vulnerabilities within 15 calendar days of initial detection.

Function 1A: 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 CM-8; NIST Cybersecurity Framework (CSF): ID.AM-1 - 4; FY 2021 CIO FISMA Metrics: 1.1, 1.1.5 and 1.4, OMB A-130, NIST SP 800-37, Rev. 2: Task P-18).

Ad Hoc (Level 1)

Comments: Auditors found the Agency's software management process lacks documented procedures for detecting and removing unapproved software on the EPA network, resulting in unapproved software installed on its region and program office networks.

Function 1A: Identify - Risk Management

2. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) 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; NIST IR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2021 CIO FISMA Metrics: 1.2, 1.3, 2.2, 3.9, CSF: ID.AM-1; NIST SP 800-37, Rev. 2: Task P-10).

Consistently Implemented (Level 3)

Comments: See remarks in question 11.2.

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: CA-7, CM-8, and CM-10; NIST SP 800-137; NIST IR 8011; FEA Framework, v2; FY 2021 CIO FISMA Metrics: 1.2.5, 1.3.3, 1.3.9, 1.3.10, 3.10; CSF: ID.AM-2; NIST SP 800-37, Rev. 2: Task P-10)?

Ad Hoc (Level 1)

Comments: Auditors found the Agency's software management process lacks documented procedures for detecting and removing unapproved software on the EPA network, resulting in unapproved software installed on its region and program office networks.

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 PM-11; NIST SP 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2021 CIO FISMA Metrics: 1.1; OMB M-19-03; NIST SP 800-37, Rev. 2: Task C-2, C-3, P-4, P-12, P-13, S-1 - S-3, NIST IR 8170)?

Consistently Implemented (Level 3)

Comments: See remarks in question 11.2.

5. To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels (NIST SP 800-39; NIST SP 800-53 Rev. 4: RA-3, PM-9; NIST IR 8286, CSF: ID.RM-1 - ID.RM-3; OMB A-123; OMB M-16-17; OMB M-17-25; NIST SP 800-37 (Rev. 2): Tasks P-2, P-3, P-14, R-2, and R-3?

Consistently Implemented (Level 3)

Comments: See remarks in question 11.2.

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 (Federal Information Technology Acquisition Reform Act (FITARA), NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2) Task P-16; OMB M-19-03; OMB M-15-14, FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-163, Rev. 1 CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

Function 1A: Identify - Risk Management

Consistently Implemented (Level 3)

Comments: See remarks in question 11.2.

7. To what extent have the roles and responsibilities of internal and external stakeholders involved in cybersecurity risk management processes been defined, communicated, and implemented across the organization (NIST SP 800-39: Section 2.3.1, 2.3.2, and Appendix D; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; NIST IR 8286, Section 3.1.1, OMB A-123; NIST SP 800-37 (Rev. 2) Section 2.8 and Task P-1; OMB M-19-03)?

Defined (Level 2)

Comments: Auditors found that EPA lacks documented procedures related to using cybersecurity registers, managing supply chain risk, and defining the types of stakeholders involved in each stage of the risk management process. Due to the Agency having corrective actions in progress to address these oversights and defined procedures for the majority of criteria assessed, auditors conclude this metric does not exceed Level 2 (Defined).

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) Task A-6, R-3; OMB M-04-14, M-19-03, CSF v1.1, ID.RA-6)?

Defined (Level 2)

Comments: Due to the corrective actions to address FY 2020 findings related to this metric having a planned completion date of December 31, 2021, the rating for FISMA Metric Question 8 remains unchanged from the previous year's rating.

9. To what extent does the organization ensure that information about cybersecurity risks is communicated in a timely and effective manner to appropriate internal and external stakeholders (OMB A-123; OMB Circular A-11 and OMB M-19-03; CSF: Section 3.3; NIST SP 800-37 (Rev. 2) Task M-5; SECURE Technology Act: s. 1326, NIST IR 8170 and 8286)?

Consistently Implemented (Level 3)

Comments: See remarks in question 11.2.

10. To what extent does the organization utilize technology/ automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123 and NIST IR 8286)?

Consistently Implemented (Level 3)

Comments: See remarks in question 11.2.

- 11.1. Please provide the assessed maturity level for the agency's Identify - Risk Management program.

Consistently Implemented (Level 3)

Comments: See remarks in question 11.2.

Function 1A: Identify - Risk Management

- 11.2. 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 limited our testing to those questions with criteria added to the metric that would materially change our FY 2020 response. If the policies, procedures, and strategies were formalized and documented, we rated the Agency at Level 3 - (Consistently Implemented). However we did not test to determine what additional steps the Agency needs to complete to achieve a higher maturity level.

Function 1B: Identify - Supply Chain Risk Management

12. To what extent does the organization utilize an organization wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services? (The Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13 Sub chap. III and Chap. 47, P.L. 115-390) (Dec. 21, 2018), NIST SP 800-53, Rev. 5, PM-30, NIST IR 8276)?

Defined (Level 2)

Comments: See remarks in question 16.3.

12. To what extent does the organization utilize an organization wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services? (The Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13 Sub chap. III and Chap. 47, P.L. 115-390) (Dec. 21, 2018), NIST SP 800-53, Rev. 5, PM-30, NIST IR 8276)?

Defined (Level 2)

Comments: See remarks in question 16.1

13. To what extent does the organization utilize SCRM policies and procedures to manage SCRM activities at all organizational tiers (The Federal Acquisition Supply Chain Security Act of 2018, NIST 800-53, Rev. 5, SR-1, NIST CSF v1.1, ID.SC-1 and ID.SC-5, NIST IR 8276)?

Defined (Level 2)

Comments: See remarks in question 16.3.

14. To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements. (The Federal Acquisition Supply Chain Security Act of 2018, NIST SP 800-53 REV. 5: SA-4, SR-3, SR-5, SR-6 (as appropriate); NIST SP 800-152; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4, NIST IR 8276).

Defined (Level 2)

Function 1B: Identify - Supply Chain Risk Management

Comments: See remarks in question 16.3.

15. To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems? (800-53 rev 5 SR-11, 11 (1), and 11(2))

Defined (Level 2)

Comments: See remarks in question 16.3.

- 16.1. Please provide the assessed maturity level for the agency's Identify - Supply Chain Risk Management program.

Defined (Level 2)

Comments: See remarks in question 16.3.

- 16.2. Please provide the assessed maturity level for the agency's Identify Function.

Consistently Implemented (Level 3)

Comments: See remarks in question 16.3.

- 16.3. Provide any additional information on the effectiveness (positive or negative) of the organization's Supply Chain 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 limited our testing to those questions with criteria added to the metric that would materially change our FY 2020 response. If the policies, procedures, and strategies were formalized and documented, we rated the Agency at Level 2 - (Defined). However we did not test to determine what additional steps the Agency needs to complete to achieve a higher maturity level.

Function 2A: Protect - Configuration Management

17. To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated, and implemented 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 remarks in question 25.2.

18. 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)

Function 2A: Protect - Configuration Management

Comments: See remarks in question 25.2.

19. 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 2021 CIO FISMA Metrics: 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1)?

Consistently Implemented (Level 3)

Comments: See remarks in question 25.2.

20. 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, RA-5, and SI-2; NIST SP 800-70, Rev. 4, FY 2021 CIO FISMA Metrics: 2.1, 2.2, 4.3; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?

Ad Hoc (Level 1)

Comments: Due to the corrective actions to address FY 2020 findings related to this metric having an planned completion date of June 30, 2022, the rating for FISMA Metric Question 20 remains unchanged from the previous year's rating.

21. 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, RA-5, SI-2, and SI-3; NIST SP 800-40, Rev. 3; SANS/CIS Top 20, Control 4.5; FY 2021 CIO FISMA Metrics: 1.3.7, 1.3.8, 2.13, 2.14; CSF: ID.RA-1; DHS Binding Operational Directives (BOD) 18-02 and 19-02)?

Ad Hoc (Level 1)

Comments: Auditor noted that the EPA has not updated its Risk Assessment or Systems and Information Integrity procedures to meet DHS BOD 19-12, Vulnerability Remediation Requirements for Internet-Accessible Systems, a federal requirement for remediating critical vulnerabilities within 15 calendar days of initial detection.

22. To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-19-26, DHS-CISA TIC 3.0 Core Guidance Documents)

Ad Hoc (Level 1)

Comments: Due to the corrective actions to address FY 2020 findings related to this metric having an planned completion date of June 30, 2022, the rating for FISMA Metric Question 20 remains unchanged from the previous year's rating.

23. 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, CM-3 and CM-4; CSF: PR.IP-3).

Ad Hoc (Level 1)

Function 2A: Protect - Configuration Management

Comments: Due to the corrective actions to address FY 2020 findings related to this metric having an planned completion date of June 30, 2022, the rating for FISMA Metric Question 20 remains unchanged from the previous year's rating.

24. To what extent does the organization utilize a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet-accessible federal systems (OMB M-20-32 and DHS BOD 20-01)?

Consistently Implemented (Level 3)

Comments: See remarks in question 25.2.

- 25.1. Please provide the assessed maturity level for the agency's Protect - Configuration Management program.

Consistently Implemented (Level 3)

Comments: See remarks in question 25.2.

- 25.2. 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 limited our testing to those questions with criteria added to the metric that would materially change our FY 2020 response. If the policies, procedures, and strategies were formalized and documented, we rated the Agency at Level 3 - (Consistently Implemented). However we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

Function 2B: Protect - Identity and Access Management

26. To what extent have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: AC-1, IA-1, and PS-1; NIST SP 800-63-3 and 800-63A, B, and C; Federal Identity, Credential, and Access Management (FICAM) playbooks and guidance (see idmanagement.gov), OMB M-19-17)?

Consistently Implemented (Level 3)

Comments: See remarks in question 34.2.

27. To what extent does the organization utilize a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities (FICAM, OMB M-19-17; NIST SP 800-53 REV. 4: AC-1 and IA-1; OMB M-19-17; SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5)?

Consistently Implemented (Level 3)

Comments: See remarks in question 34.2.

28. To what extent has the organization developed and implemented processes for assigning position risk designations and performing

Function 2B: Protect - Identity and Access Management

appropriate personnel 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, OMB M-19-17)?

Consistently Implemented (Level 3)

Comments: See remarks in question 34.2.

29. 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 PS-6)?

Consistently Implemented (Level 3)

Comments: See remarks in question 34.2.

30. To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for non-privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access (HSPD-12; NIST SP 800-53 REV. 4: AC-17, IA-2, IA-5, IA-8, and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63, 800-157; FY 2021 CIO FISMA Metrics: 2.4, 2.7, CSF: PR.AC-1 and 6; OMB M-19-17, and NIST SP 800-157)?

Consistently Implemented (Level 3)

Comments: See remarks in question 34.2.

31. To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access (HSPD-12; NIST SP 800-53 REV. 4: AC-17, PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63 and 800-157; OMB M-19-17, FY 2021 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; and DHS ED 19-01)?

Consistently Implemented (Level 3)

Comments: See remarks in question 34.2.

32. 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 2021 CIO FISMA Metrics: 2.3, 2.5, 2.6, and 2.7; OMB M-19-17, NIST SP 800-53 REV. 4: AC-1, AC-2, AC-5, AC-6, AC-17; AU-2, AU-3, AU-6, and IA-4; DHS ED 19-01; CSF: PR.AC-4).

Consistently Implemented (Level 3)

Comments: See remarks in question 34.2.

Function 2B: Protect - Identity and Access Management

33. 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-11, AC-12, AC-17, AC-19, AU-2, IA-7, SC-10, SC-13, and SI-4; CSF: PR.AC-3; and FY 2021 CIO FISMA Metrics: 2.10 and 2.11).

Defined (Level 2)

Comments: Due to the corrective actions to address FY 2020 findings related to this metric having an planned completion date of December 31, 2021, the rating for FISMA Metric Question 33 remains unchanged from the previous year's rating.

- 34.1. Please provide the assessed maturity level for the agency's Protect - Identity and Access Management program.

Consistently Implemented (Level 3)

Comments: See remarks in question 34.2.

- 34.2. 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 limited our testing to those questions with criteria added to the metric that would materially change our FY 2020 response. If the policies, procedures, and strategies were formalized and documented, we rated the Agency at Level 3 - (Consistently Implemented). However we did not test to determine what additional steps the Agency needs to complete to achieve a higher maturity level.

Function 2C: Protect - Data Protection and Privacy

35. 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) Section 2.3, Task P-1 ; OMB M-20-04; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J, FY 2020 SAOP FISMA metrics, Sections 1 through 4, 5(b), NIST Privacy Framework)?

Consistently Implemented (Level 3)

Comments: See remarks in question 40.2.

36. 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 2021 CIO FISMA Metrics: 2.8, 2.12; 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

Function 2C: Protect - Data Protection and Privacy

·Sanitization of digital media prior to disposal or reuse

Consistently Implemented (Level 3)

Comments: See remarks in question 40.2.

37. 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 2021 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?

Consistently Implemented (Level 3)

Comments: See remarks in question 40.2.

38. 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 2020 SAOP FISMA metrics, Section 12; OMB M-17-12; and OMB M-17-25)?

Consistently Implemented (Level 3)

Comments: See remarks in question 40.2.

39. To what extent 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, FY 2020 SAOP FISMA Metrics, Sections 9 10, and 11)?

Consistently Implemented (Level 3)

Comments: See remarks in question 40.2.

- 40.1. Please provide the assessed maturity level for the agency's Protect - Data Protection and Privacy program.

Consistently Implemented (Level 3)

Comments: See remarks in question 40.2.

- 40.2. 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 limited our testing to those questions with criteria added to the metric that would materially change our FY 2020 response. If the policies, procedures, and strategies were formalized and documented, we rated the Agency at Level 3 - (Consistently Implemented). However we did not test to determine what additional steps the Agency needs to complete to achieve a higher maturity level.

Function 2D: Protect - Security Training

41. To what extent have the roles and responsibilities of security awareness and training program stakeholders been defined,

Function 2D: Protect - Security Training

communicated, and implemented 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 remarks in question 46.3.

42. 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 remarks in question 46.3.

43. To what extent does the organization utilize a security awareness and training strategy/plan that leverages its skills assessment and is adapted to its mission and risk environment? (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 remarks in question 46.3.

44. To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, 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-1, AT-2; FY 2021 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 remarks in question 46.3.

45. To what extent does the organization ensure that specialized security training is provided to individuals with significant security responsibilities (as defined in the organization's security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301) (NIST SP 800-53 REV. 4: AT-3 and AT-4; FY 2021 CIO FISMA Metrics: 2.15, and 5 Code of Federal Regulation 930.301)?

Function 2D: Protect - Security Training

Consistently Implemented (Level 3)

Comments: See remarks in question 46.3.

- 46.1. Please provide the assessed maturity level for the agency's Protect - Security Training program.

Consistently Implemented (Level 3)

Comments: See remarks in question 46.3.

- 46.2. Please provide the assessed maturity level for the agency's Protect function.

Consistently Implemented (Level 3)

Comments: See remarks in question 46.3.

- 46.3. 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 limited our testing to those questions with criteria added to the metric that would materially change our FY 2020 response. If the policies, procedures, and strategies were formalized and documented, we rated the Agency at Level 3 - (Consistently Implemented). However we did not test to determine what additional steps the Agency needs to complete to achieve a higher maturity level.

Function 3: Detect - ISCM

47. To what extent does the organization utilize information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier (NIST SP 800-37 (Rev. 2) Task P-7; NIST SP 800-137: Sections 3.1 and 3.6)?

Consistently Implemented (Level 3)

Comments: See remarks in question 51.2.

48. To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization (NIST SP 800-53 REV. 4: CA-1; NIST SP 800-137; CSF: DE.DP-1; NIST 800-37, Rev. 2 Task P-7 and S-5)

Consistently Implemented (Level 3)

Comments: See remarks in question 51.2.

49. How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls (OMB A-130, 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

Function 3: Detect - ISCM

Authorization; NIST SP 800-37 (Rev. 2) Task S-5; NIST SP 800-18, Rev. 1, NIST IR 8011; OMB M-14-03; OMB M-19-03)

Consistently Implemented (Level 3)

Comments: See remarks in question 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 remarks in question 51.2.

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

Consistently Implemented (Level 3)

Comments: See remarks in question 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 limited our testing to those questions with criteria added to the metric that would materially change our FY 2020 response. If the policies, procedures, and strategies were formalized and documented, we rated the Agency at Level 3 - (Consistently Implemented). However we did not test to determine what additional steps the Agency needs to complete to achieve a higher maturity level.

Function 4: Respond - Incident Response

52. To what extent does the organization utilize an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents (NIST SP 800-53 REV. 4: IR-8; NIST SP 800-61 Rev. 2, section 2.3.2; CSF, RS.RP-1, Presidential Policy Directive (PPD) 8 - National Preparedness)?

Consistently Implemented (Level 3)

Comments: See remarks in question 59.2.

52. To what extent does the organization utilize an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents (NIST SP 800-53 REV. 4: IR-8; NIST SP 800-61 Rev. 2, section 2.3.2; CSF, RS.RP-1, Presidential Policy Directive (PPD) 8 - National Preparedness)?

Consistently Implemented (Level 3)

Comments: See remarks in question 59.2.

53. To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and

Function 4: Respond - Incident Response

dependencies been defined, communicated, and implemented across the organization (NIST SP 800-53 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; CSF, RS.CO-1, OMB M-20-04; FY 2021 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?

Consistently Implemented (Level 3)

Comments: See remarks in question 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-20-04; CSF: DE.AE-1, DE.AE-2 -5, PR.DS-6, RS.AN-1 and 4, and PR.DS-8; and US-CERT Incident Response Guidelines)

Consistently Implemented (Level 3)

Comments: See remarks in question 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 remarks in question 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-20-04; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 5; DHS Cyber Incident Reporting Unified Message)

Consistently Implemented (Level 3)

Comments: See remarks in question 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-20-04; PPD-41).

Consistently Implemented (Level 3)

Comments: See remarks in question 59.2.

58. To what extent 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

Function 4: Respond - Incident Response

File integrity and endpoint and server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2; NIST SP 800-44)

Consistently Implemented (Level 3)

Comments: See remarks in question 59.2.

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

Consistently Implemented (Level 3)

Comments: See remarks in question 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 limited our testing to those questions with criteria added to the metric that would materially change our FY 2020 response. If the policies, procedures, and strategies were formalized and documented, we rated the Agency at Level 3 - (Consistently Implemented). However we did not test to determine what additional steps the Agency needs to complete to achieve a higher maturity level.

Function 5: Recover - Contingency Planning

60. To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined, communicated, and implemented across the organization, including appropriate delegations of authority (NIST SP 800-53 REV. 4: CP-1, CP-2, and CP-3; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?

Consistently Implemented (Level 3)

Comments: See remarks in question 66.2.

61. To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; NIST IR 8286; FIPS 199; FCD-1; OMB M-19-03; FY 2021 CIO FISMA Metrics, Section 5; CSF:ID.RA-4)?

Consistently Implemented (Level 3)

Comments: See remarks in question 66.2.

62. 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 2021 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?

Consistently Implemented (Level 3)

Comments: See remarks in question 66.2.

Function 5: Recover - Contingency Planning

63. 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 2021 CIO FISMA Metrics, Section 5; CSF: ID.SC-5 and CSF: PR.IP-10)?

Consistently Implemented (Level 3)

Comments: See remarks in question 66.2.

64. 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 2021 CIO FISMA Metrics, Section 5; and NARA guidance on information systems security records)?

Consistently Implemented (Level 3)

Comments: See remarks in question 66.2.

65. 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 remarks in question 66.2.

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

Consistently Implemented (Level 3)

Comments: See remarks in question 66.2.

- 66.2. 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 limited our testing to those questions with criteria added to the metric that would materially change our FY 2020 response. If the policies, procedures, and strategies were formalized and documented, we rated the Agency at Level 3 - (Consistently Implemented). However we did not test to determine what additional steps the Agency needs to complete to achieve a higher maturity level.

APPENDIX A: Maturity Model Scoring

A.1. Please provide the assessed maturity level for the agency's Overall status.

Function 1A: Identify - Risk Management

Function	Count
Ad-Hoc	2
Defined	2
Consistently Implemented	6
Managed and Measurable	0
Optimized	0
<hr/>	
Calculated Rating: Consistently Implemented (Level 3)	
Assessed Rating: Consistently Implemented (Level 3)	

Function 1B: Identify - Supply Chain Risk Management

Function	Count
Ad-Hoc	0
Defined	4
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
<hr/>	
Calculated Rating: Defined (Level 2)	
Assessed Rating: Defined (Level 2)	

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	4

APPENDIX A: Maturity Model Scoring

Defined	0
Consistently Implemented	4
Managed and Measurable	0
Optimized	0
<hr/>	
Calculated Rating: Consistently Implemented (Level 3)	
Assessed Rating: Consistently Implemented (Level 3)	

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	7
Managed and Measurable	0
Optimized	0
<hr/>	
Calculated Rating: Consistently Implemented (Level 3)	
Assessed Rating: Consistently Implemented (Level 3)	

Function 2C: Protect - Data Protection and Privacy

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	5
Managed and Measurable	0
Optimized	0
<hr/>	
Calculated Rating: Consistently Implemented (Level 3)	

APPENDIX A: Maturity Model Scoring

Assessed Rating: Consistently Implemented (Level 3)

Function 2D: Protect - Security Training

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	5
Managed and Measurable	0
Optimized	0
Calculated Rating: Consistently Implemented (Level 3)	
Assessed Rating: Consistently Implemented (Level 3)	

Function 3: Detect - ISCM

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	4
Managed and Measurable	0
Optimized	0
Calculated Rating: Consistently Implemented (Level 3)	

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	0

APPENDIX A: Maturity Model Scoring

Consistently Implemented	7
Managed and Measurable	0
Optimized	0
<hr/>	
Calculated Rating: Consistently Implemented (Level 3)	

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	6
Managed and Measurable	0
Optimized	0
<hr/>	
Calculated Rating: Consistently Implemented (Level 3)	

Overall

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management / Supply Chain Risk Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	See remarks in question 16.3.
Function 2: Protect - Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	See remarks in question 46.3.
Function 3: Detect - ISCM	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	See remarks in question 51.2.
Function 4: Respond - Incident Response	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	See remarks in question 59.2.

APPENDIX A: Maturity Model Scoring

Function 5: Recover - Contingency Planning	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	See remarks in question 66.2.
Overall	Not Effective	Effective	See remarks in question 0.2.

Information Security Reports Issued in FY 2021

The EPA OIG issued the following reports in FY 2021, which included recommendations regarding improvements within the EPA's information security program:

- Report No. [21-E-0031](#)**, *EPA Needs to Improve Oversight of Invoice Reviews and Contractor Performance Evaluation*, issued December 1, 2020. We concluded that the EPA did not perform certain contract management duties that pertain to overseeing invoice review during the task order's base year period and contractor performance evaluation. As a result, the EPA reviewed the January 2019 invoice, valued at \$22,533, after we brought the lack of periodic invoice reviews to the contracting officer's attention. We issued this report on these weaknesses because effective contract management practices safeguard the EPA from remitting costs that are not allowable, allocable, and reasonable. The Agency agreed with the recommendations and completed corrective actions for Recommendation 3. Recommendations 1, 2, 4, and 5 are considered resolved with corrective actions pending.
- Report No. [21-E-0124](#)**, *EPA Needs to Improve Processes for Updating Guidance, Monitoring Corrective Actions, and Managing Remote Access for External Users*, issued April 16, 2021. We concluded that the EPA has deficiencies in the following areas: (1) completing reviews of outdated information security procedures by the established deadlines, (2) verifying corrective actions are completed as represented by the Agency and not falsely reporting related resolutions, and (3) enforcing established information system control requirements for the Agency's web application directory system. Deficiencies in the EPA's IT internal controls could be used to exploit weaknesses in Agency applications and to hinder the EPA's ability to prevent, detect, and respond to emerging cyberthreats. The Agency agreed with the recommendations and completed corrective actions for Recommendations 2 and 5. Recommendations 1, 3, and 4 are considered resolved with corrective actions pending.
- Report No. [21-E-0226](#)**, *EPA's Emergency Response Systems at Risk of Having Inadequate Security Controls*, issued September 13, 2021. We concluded that the EPA's security-categorization process did not include key participants as recommended by the National Institute of Standards and Technology. In addition, security documentation for some of the EPA's minor applications did not exist. The National Institute of Standards and Technology requires agencies to develop system security plans for all information systems, including major applications and general support systems, and to tailor the systems' security controls based on the systems' security categorization. We issued this report on these issues because the availability and integrity of emergency response system data may harm the EPA's ability to coordinate response efforts to protect the public from environmental disasters. The Agency agreed with the recommendations and completed corrective actions for Recommendations 1, 2, 3, 6, and 7. Recommendations 4 and 5 are considered resolved with corrective actions pending.
- Report No. [21-P-0241](#)**, *EPA Effectively Planned for Future Remote Access Needs but Should Disconnect Unneeded Services in Timely Manner*, issued September 20, 2021. We concluded that the EPA did not disconnect U.S. General Services Administration services, such as analog phone and digital subscriber lines, that were no longer needed in a timely manner. Specifically, as part of its Enterprise Infrastructure Solutions transition activities, which began in 2015, the EPA identified unneeded General Services Administration services, but as of May 2021, 268 of the

services determined to be unneeded were still not disconnected. Because the EPA has taken steps to disconnect unneeded services as part of its Enterprise Infrastructure Solutions transition activities, we made no recommendations regarding this finding.

EPA FY 2021 FISMA Compliance Results

Table D-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
Identify	Supply Chain Risk Management	Level 2: Defined
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
The EPA's overall maturity rating: Level 3 (Consistently Implemented)		

Source: OIG test results. (EPA OIG table)

Table D-2: EPA FISMA metrics that need improvement

Security function	Security domain	Explanation of metrics areas that need improvement
Identify	Risk Management	The EPA's software management process lacks documented procedures for detecting and removing unapproved software on the EPA network, resulting in unapproved software installed on its region and program office networks (Appendix A, metric questions 1 and 3).

Source: OIG test results. (EPA OIG table)

Agency Response to Draft Report



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

March 18, 2022

OFFICE OF MISSION SUPPORT

MEMORANDUM

SUBJECT: Response to Office of Inspector General Draft Report *"EPA Lacks Documented Procedures for Detecting and Removing Unapproved Software and Remediating Critical Vulnerabilities on Agency Network"* Project No. OA-FY21-0206 dated January 25, 2022

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

TO: LaSham Barnes, Director
Information Resources Management Directorate
Office of Audit

Digitally signed by
VAUGHN NOGA
Date: 2022.03.18
12:59:18 -04'00'

Thank you for the opportunity to respond to the issues and recommendations in the subject audit document. Following is a summary of the agency's overall position, along with each of the report recommendations. For those report recommendations with which the Agency agrees we have provided high-level intended corrective actions and estimated completion dates.

The Office of Mission Support/Office of Information Security and Privacy (OMS/OISP) concurs with the recommendations outlined in the Office of Inspector General's Draft Report and has developed two corrective actions to address them. Those corrective actions are outlined in the corrective action plan below.

You will note that OMS did not propose a corrective action to address recommendation 1. The recommendation was discussed at the exit conference on February 8th. Following the meeting, Jeremy Sigel sent an email (attached) to Marilyn Armstrong stating:

"As a result of the exit conference discussions we agree that the Agency's current critical vulnerability remediation timeframes are more stringent than the DHS BOD update and therefore will be removing that language from the Final Report. As such, Recommendation #1 does not require a Corrective Action Plan response from the Agency. We will just proceed with Recommendations 2 and 3. Thank you for the feedback and your understanding."

OMS RESPONSE TO REPORT RECOMMENDATIONS

No:	Recommendation	High Level Intended Corrective Actions	Estimated Completion Date
2	Develop and document procedures for detecting and removing unapproved software on the Agency's network to include time frames for removal, risk classifications, and identification of software collecting privacy data.	OMS has developed and disseminated policies and procedures for software management. The policy, <u>Software Management and Piracy Policy</u> (CIO 2104.2) and the procedure <u>Software Management and Piracy Procedure</u> (CIO 2104-P-01.1) requires that only software approved and properly acquired be installed on EPA computer systems. OMS recognizes that the procedure can be updated to clearly outline the current processes for software certification, as well as, the identification and removal of unapproved software from EPA's network and will complete the update accordingly.	October 31, 2022
3	Develop and provide training on the Agency's processes for detecting and removing unapproved software to users with privileges to install software on the EPA's network.	OMS will provide training on the process for detecting and removing unapproved software to users assigned the related privileges, roles and responsibilities.	January 31, 2023

Thank you for the opportunity to review the report. If you have any questions regarding this response, please contact Daniela Wojtalewicz, Audit Follow-up Coordinator, of the Office of Resources and Business Operations, (202) 564-2849 or wojtalewicz.daniela@epa.gov.

Attachment

cc: LaVonda Harris-Claggett
Eric Jackson Jr.
Alonzo Munyeneh
Jeremy Sigel
Sabrena Stewart

Erin Collard
David Alvarado
Austin Henderson
Tonya Manning
Lee Kelly
Mark Bacharach
James Hunt
Dan Coogan
Jan Jablonski
Marilyn Armstrong
Daniela Wojtalewicz
Afreeka Wilson
Andrew LeBlanc
Jose Kercado-Deleon

Distribution

The Administrator
Deputy Administrator
Chief of Staff, Office of the Administrator
Deputy Chief of Staff, Office of the Administrator
Deputy Chief of Staff for Operations, 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
Deputy Assistant Administrator for Mission Support
Deputy Assistant Administrator for Environmental Information and Chief Information Officer, Office of Mission Support
Director, Office of Continuous Improvement, Office of the Chief Financial Officer
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