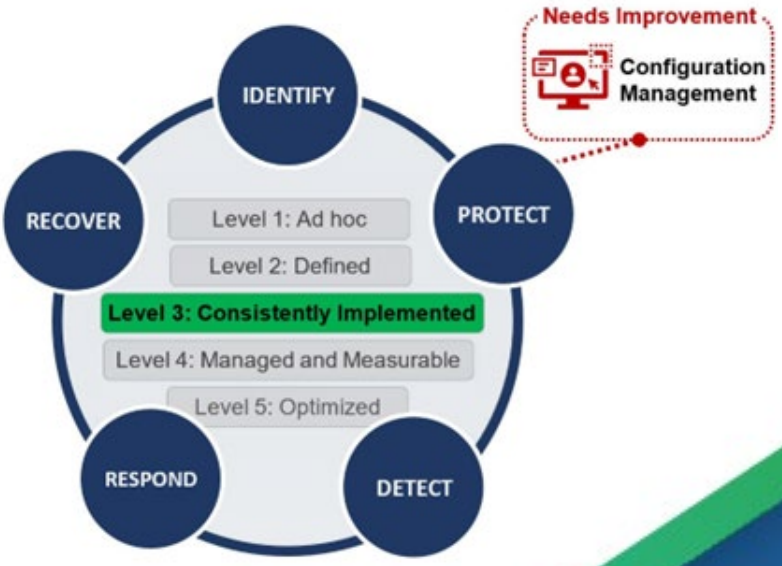
The EPA's Vulnerability Tracking and Remediation and Information Technology Procedures Review Processes Are Implemented Inconsistently

July 5, 2023 | Report No. 23-E-0021



OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

Report Contributors:

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

Abbreviations:

ARadDS	Analytical Radiation Data System
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
NIST	National Institute of Standards and Technology
OAR	Office of Air and Radiation
OIG	Office of Inspector General
OMB	Office of Management and Budget
OMS	Office of Mission Support
POA&M	Plan of Action and Milestone
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 the configuration management security domain needs improvement. (EPA OIG image)

Are you aware of fraud, waste, or abuse in an EPA program?

EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW (2431T)
Washington, 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

23-E-0021
July 5, 2023

The EPA's Vulnerability Tracking and Remediation and Information Technology Procedures Review Processes Are Implemented Inconsistently

Why We Did This Evaluation

To accomplish this objective:

The U.S. Environmental Protection Agency Office of Inspector General conducted this evaluation to assess the EPA's compliance with the fiscal year 2022 inspector general reporting metrics for the Federal Information Security Modernization Act of 2014.

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).

To support these EPA mission-related efforts:

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

To address this top EPA management challenge:

- *Protecting EPA systems and other critical infrastructure against cyberthreats.*

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

List of OIG reports.

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 2022 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 the following areas:

Without timely tracking and remediation of known vulnerabilities, the Agency risks compromising the confidentiality, integrity, and availability of environmental and radiation data used for determining responses to national incidents and safeguarding first responder personnel.

- Updating information security procedures in a timely manner to meet the requirements of National Institute of Standards and Technology publications within one year of their publication.
- Tracking and remediating vulnerabilities identified for the Analytical Radiation Data System in a timely manner.

Recommendations and Planned Agency Corrective Actions

We recommend that the assistant administrator for Mission Support develop a process to keep information security procedures consistent with the most current revision of the National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*. Additionally, we recommend that the assistant administrator for Air and Radiation develop, implement, and assign responsibilities for a plan to prioritize and schedule installation of patches that address critical vulnerabilities in the Analytical Radiation Data System within Agency required time frames. The Agency agreed with our recommendations and provided acceptable planned corrective actions with estimated milestone dates. We consider the recommendations resolved with corrective actions pending.

OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

July 5, 2023

MEMORANDUM

SUBJECT: The EPA's Vulnerability Tracking and Remediation and Information Technology Procedures Review Processes Are Implemented Inconsistently
Report No. 23-E-0021

FROM: Sean W. O'Donnell, Inspector General

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

Joseph Goffman, Principal Deputy Assistant Administrator
Office of Air and Radiation

This is our report on the subject evaluation conducted by the U.S. Environmental Protection Agency Office of Inspector General. The project number for this evaluation was OA-FY22-0134. 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 and the Office of Air and Radiation are 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

Appendixes

Chapter 1
Introduction

Purpose

The U.S. Environmental Protection Agency Office of Inspector General initiated this evaluation to assess the EPA's compliance with the fiscal year 2022 inspector general reporting requirements for the Federal Information Security Modernization Act of 2014.

Top Management Challenge

This evaluation addresses the following top management challenge for the Agency, as identified in the OIG's *U.S. Environmental Protection Agency Fiscal Year 2023 Top Management Challenges* report, issued October 28, 2022:

- Protecting EPA systems and other critical infrastructure against cyberthreats.

Background

Under FISMA, agency heads are responsible for protecting information systems and information collected, maintained, or used by or on behalf of their respective agencies. The information security protections must be commensurate with the risk of harm that would result from the unauthorized access, use, disclosure, disruption, modification, or destruction of the agency information or information systems.[1] FISMA further requires that inspectors general conduct an annual evaluation to assess the effectiveness of their respective agencies' information security program and practices.[2]

The Office of Management and Budget, in coordination with the Counsel of the Inspectors General on Integrity and Efficiency and other federal partners, issued guidance for inspectors general to implement FISMA requirements. For fiscal year 2022 reporting, the OMB issued M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*, dated December 6, 2021. For inspectors general to implement this guidance, the OMB issued the *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*, which supplemented and expanded upon the OMB's *FY 2022 Core IG FISMA Metrics Evaluation Guide*. These OMB inspector general guidance documents are collectively referred to as the FY 2022 Core IG Metrics.

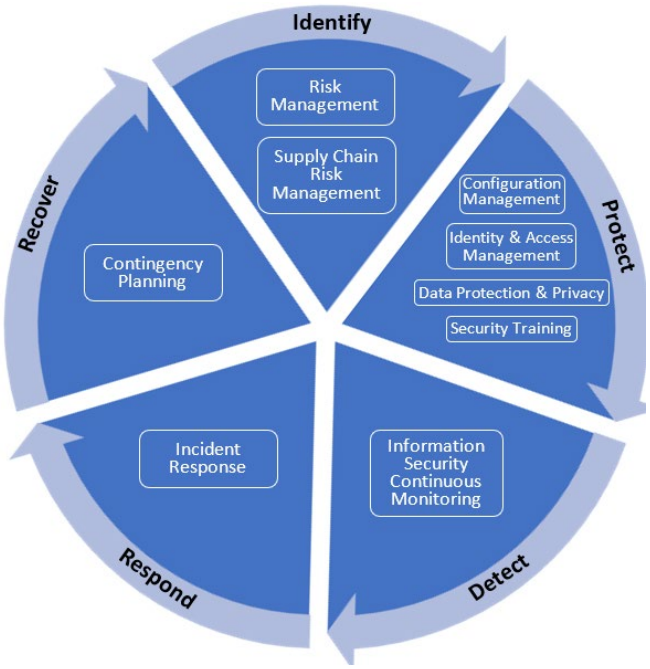
The FY 2022 Core IG Metrics are aligned to the five function areas identified in the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, dated April 16, 2018. Identify, protect, detect, respond, and recover are the five function areas identified in the framework. Referred to as the *Cybersecurity Framework*, this NIST publication provides agencies with a common structure for assessing cybersecurity capabilities and associated risks across the enterprise and gives IGs a foundation for communicating capabilities and the maturity of controls that support them.

The inspector general metrics focus on key areas to ensure successful independent evaluation of the agency's information security. As noted in the FY 2022 Core IG metrics, the metrics selected for FY 2022

[1] 44 U.S.C. § 3554(a)(1)(A).
[2] 44 U.S.C. § 3555(b)(1).

were chosen to align with Executive Order 14028, *Improving the Nation's Cybersecurity*, dated May 12, 2021, as well as OMB guidance to agencies to further federal cybersecurity modernization. The FY 2022 Core IG Metrics provide 20 core metrics, listed in Appendix B, to assess across the five function areas' nine domains, shown in Figure 1, to provide sufficient data for determining the effectiveness of an Agency's information security program with a high level of confidence.

Figure 1: FY 2022 cybersecurity framework—five security functions with nine security domains



Source: OIG summary of the FY 2022 Core IG Metrics.
(EPA OIG image)

The assessment of effectiveness of an agency's information security program is based on a five-tiered maturity model spectrum, illustrated in Figure 2. Each IG is responsible for annually assessing the agency's rating along this spectrum by determining to what degree the agency implements 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 in the FY 2022 Core IG Metrics template.

Figure 2: Maturity model spectrum

Note: Though the source for this model is from FY 2021, the FY 2022 Core IG Metrics state that they are using the maturity model spectrum identified in prior inspector general FISMA guidance.

Source: *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.1, dated May 12, 2021. (EPA OIG image)

The maturity model spectrum identifies the levels at which an agency has developed policies and procedures at the foundational levels and advanced maturity levels when it has fully institutionalized those policies and procedures. While IGs can base the determination of effectiveness on the results of the metrics assessment, the FY 2022 IG Core Metrics state that they should consider "their own assessment of the unique missions, resources, and challenges" their agencies face when assessing the maturity of information security programs.

In addition to the above guidance, OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, dated July 15, 2016, states that management is responsible for establishing and integrating internal control into its operations in such a manner as to provide reasonable assurance that the entity's internal control over operations, reporting, and compliance are operating effectively. Such controls would include the information security policies and procedures that the FY 2022 IG Core Metrics are designed to assess.

Responsible Offices

The Office of Air and Radiation, or the OAR, develops national programs, policies, and regulations for controlling air pollution and radiation exposure. It controls the use of the Analytical Radiation Data System, or ARadDS, which we reviewed. The ARadDS lab is located within the OAR's Office of Radiation and Indoor Air. The ARadDS roles within the OAR are identified as:

- The system owner, who is responsible for the operation of the system.
- The authorizing official, who is responsible for approving the security implementation of the system.

The chief information security officer in the Office of Mission Support, or the OMS, provides technical and managerial assistance for the ARadDS. Additionally, the Office of Information Security and Privacy within the OMS promotes agencywide cooperation in managing risks and protecting EPA information. It also defines clear, comprehensive, and enterprisewide information security and privacy strategies.

Scope and Methodology

We conducted this evaluation from May 2022 to June 2023 in accordance with the *Quality Standards for Inspection and Evaluation* published in December 2020 by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we perform the evaluation to obtain sufficient and appropriate evidence to support our findings.

We assessed the EPA using the criteria and analysis that the FY 2022 IG Core Metrics require for Level 3 (Consistently Implemented) for the domains within each FISMA security function area, which denotes that its policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking. If the Agency's policies, procedures, and strategies were not consistently implemented, we rated that metric at Level 2 (Defined).

Additionally, we reviewed the information security reports that we or the U.S. Government Accountability Office issued in FY 2022 to identify weaknesses related to the FY 2022 FISMA metrics, as seen in Appendix C. We conducted a risk assessment using the FY 2022 Core IG Metrics and the results of our FY 2021 FISMA evaluation of the overall effectiveness of the EPA's information security posture. We defined a metric as low risk if our FY 2021 FISMA assessment resulted in a finding related to the metric and a corrective action was pending during our FY 2022 evaluation.

For all other high-risk metrics, we inquired with Agency personnel, inspected relevant Agency IT documentation, and analyzed evidence supporting the EPA's compliance with the metrics outlined in the FY 2022 Core IG Metrics. We also requested the EPA's listing of High Value Assets, from which we selected the only system the EPA's Risk Management Framework tool categorized as high impact: the ARadDS. We assessed controls around the selected system for those metrics targeted at the system level.

We provided the Agency our assessment of each function area of the FY 2022 Core IG Metrics and discussed the results. We submitted our assessment for each of the 20 core metrics from the FY 2022 IG Core Metrics, which is in Appendix D, to the OMB on July 28, 2022.

Prior Reports

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. When the report was issued, two of the recommendations were completed and the remaining three were considered resolved with planned corrective actions pending. While we verified that the Agency completed corrective actions for two of the three remaining recommendations, corrective actions for Recommendation 1 related to keeping information security procedures consistent with current federal directives, with a planned completion date of June 30, 2022, had not been completed as of August 2022. While the Agency revised the planned completion date for Recommendation 1 to November 15, 2022, that recommendation remains open. Additionally, during our FY 2022 FISMA assessment, we found that multiple other information security procedures documents were outdated and not compliant with federal directives. We discuss these additional Agency procedures within Chapter 2 of this report.

Our FY 2021 FISMA evaluation in Report No. 22-E-0028, *The EPA Lacks Documented Procedures for Detecting and Removing Unapproved Software on the Agency's Network*, issued March 30, 2022, contained two recommendations we considered resolved. We confirmed that the Agency updated *Software Management and Piracy Procedure*, CIO 2104-P-01.2, to outline processes for the identification and removal of unapproved software in fulfillment of Recommendation 1. The chief information officer approved this document on December 20, 2022, and it was posted on the EPA intranet for distribution to relevant personnel.

Results

We concluded that the EPA achieved an overall maturity level of Level 3 (Consistently Implemented) for the five security functions outlined in the *FY 2022 IG Core FISMA Metrics*, which are listed in Appendix E. This 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 deficiencies in the following areas:

- Untimely review of policies and procedures to remain current with federal requirements.
- Not tracking or remediating identified vulnerabilities in ARadDS in a timely manner.

See Chapters 2 and 3 for a detailed analysis of the above findings.

Chapter 2
EPA IT Procedures Are Not Timely Updated to Comply with Federal Requirements

During our analysis of the FY 2022 Core IG Metrics, we used Agency information technology procedures to evaluate compliance with federal requirements and guidance. We noted that those procedures were outdated and did not comply with OMB requirements. This occurred because the Agency's procedure allows three years after the issuance date for CIO directives to be reviewed for updating, while the OMB requires agencies to comply with NIST standards and guidelines within one year of their publication. Although the outdated procedures did not affect the overall classification for the domain area, not having timely updated information directives that comply with NIST standards puts the Agency's information and information systems at risk of being able to adequately support the EPA's operations and assets.

EPA IT Procedures Are Not Reviewed and Updated Within Federally Required Time Frames

OMB Circular A-130, *Managing Information as a Strategic Resource*, dated July 28, 2016, states that for information systems already in place, agencies are expected to comply with NIST standards and guidelines within one year of their respective publication dates unless otherwise directed by the OMB. However, CIO 2190.0-P-01.0, *Reviewing and Updating Agencywide Directives Administered by the EPA CIO*, dated November 4, 2013, states that CIO directives are assigned a review date, which is generally only every three years, to signify when a review of the directive is warranted. This procedure also states that a directive may be reviewed at any time to determine whether it is up to date and meets federal mandates.

In our assessment of the EPA's compliance with FY 2022 Core IG Metrics, we found that the EPA has not updated several IT procedures covering the Agency's implementation of security control requirements, including those of NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 5, dated December 2020. The latest version of NIST Special Publication 800-53, Revision 5, at the time of our evaluation was Revision 5; however, the Agency IT procedures noted in Table 1 all state implementation of Revision 4 or earlier.

Table 1: Agency IT procedure documents not timely updated

Procedure	Related cybersecurity framework security function and core IG metric number*	CIO approval date	Planned review date	Months since planned review date as of February 2023
CIO 2150-P-14.2 *Information Security – Risk Assessment Procedures*	Identify—5,10	4/11/16	4/11/19	46
CIO 2150-P-23.1 *Information Security – Program Management Procedures*	Identify—5,10	August 2019	August 2021	18
CIO 2150-P-01.2 *Information Security – Access Control Procedures*	Protect—32	9/21/15	9/21/18	53

Procedure	Related cybersecurity framework security function and core IG metric number*	CIO approval date	Planned review date	Months since planned review date as of February 2023
CIO 2150.3-P-16.1 *Information Security – Interim System and Communications Protection Procedures*	Protect—36	8/6/12	8/6/15	90
CIO 2150-P-10.2 *Information Security – Media Protection Procedures*	Protect—36	1/8/16	1/8/19	49
CIO 2150-P-17.2 *Information Security – Interim System and Information Integrity Procedures*	Protect—37	1/17/17	None stated	N/A
CIO 2150-P-02.2 *Information Security – Awareness and Training Procedures*	Protect—42	2/16/16	2/16/19	48
CIO 2150-P-04.2 *Information Security – Security Assessment and Authorization Procedures*	Detect—49	5/27/16	5/27/19	45
CIO-2150-P-08.2 *Information Security – Incident Response Procedures*	Respond—54	11/30/15	11/30/18	50
CIO 2150-P-06.2 *Information Security – Contingency Planning Procedures*	Respond - 55 Recover—61, 63	9/11/15	9/11/18	51

Source: OIG summary of EPA IT directives used for the FY 2022 assessment that were not timely updated. (EPA OIG table)

* Core IG metric numbers are identified in Appendix B.

As illustrated in Table 1, Agency procedures across many key security control families, such as risk assessment, configuration management, access controls, system and information integrity, contingency planning, and incident response, have gone months and years without an update to adhere to current NIST standards and procedures. While the reviews and planned completion dates to update the IT security control procedures are being tracked in plans of actions and milestones, or POA&Ms, the procedures continue to be outdated. We previously reported on similar issues in the FY 2020 EPA FISMA report issued April 16, 2021. In that report, we recommended that the Agency update information security procedures to make them consistent with the latest federal directives. The Agency provided acceptable corrective actions to address the recommendation with a planned completion date of June 30, 2022. As of August 2022, the Agency was unable to provide support that these actions were completed and updated the Agency's tracking system with a revised planned completion date of November 15, 2022. However, as of March 2023, the corrective actions are still recorded as active in the Agency's report tracking system.

A **POA&M** is a document that identifies tasks to be accomplished to address vulnerabilities. It details the resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

OMB Circular A-123 requires that the EPA maintain updated internal controls, such as information security procedures, for its programs. While the Agency's CIO 2190.0-P-01.0 has documented procedures that implement internal controls for updating its information security procedures, that directive provides that directives be assigned review dates which are generally three years after its initial approval. This incongruence with the OMB's one-year requirement caused the Agency's procedures to go years without finalizing an updated information directive. Without a process in place to review and update IT security control procedures documentation within required federal time frames, the Agency cannot ensure that the information security program adheres to the latest federal

requirements for implementing the information system security controls needed to protect the confidentiality, integrity, and availability of the EPA systems and data.

Recommendations

We recommend that the assistant administrator for Mission Support:

1. Update CIO 2190.0-P-01.0, *Reviewing and Updating Agencywide Directives Administered by the EPA CIO*, to include a timely process for reviewing and updating information security procedures within a year of the issuance of relevant National Institute of Standards and Technology publications.

Agency Response and OIG Assessment

The OMS agreed with the OIG's findings and the intention of Recommendation 1 to update its procedures for reviewing CIO directives in accordance with NIST publications. However, the OMS proposed a broader corrective action for updating its procedures that incorporates federal mandates and guidance in addition to NIST publications. We believe that the proposed corrective action will satisfy the intent of the recommendation. Therefore, we consider Recommendation 1 resolved with corrective action pending. Appendix F contains the OMS's response to the draft report.

Chapter 3
The EPA Failed to Address Vulnerabilities Within Required Time Frames

The OAR has not consistently deployed patches to remediate vulnerabilities in a timely manner. Specifically, we found that vulnerabilities identified for ARadDS during our FY 2022 FISMA assessment were not being remediated within Agency-required time frames, and the POA&Ms were not being created to track the resolution of vulnerabilities that are not remediated within those required time frames. The EPA information directives require remediation of vulnerabilities within two to 30 days, depending on their severity. Additionally, Agency procedures require the development of POA&Ms to manage flaw remediation in the Agency's reporting and tracking tool. By not adhering to its required time frames addressing vulnerabilities in the patch mitigation process, the Agency puts its environmental and radiation data at risk of being exploited by threats.

The OAR Did Not Remediate Vulnerabilities in a Timely Manner

Vulnerabilities for ARadDS were not being remediated in a timely manner and as prescribed by EPA procedures. We found that patches to remediate vulnerabilities had not been applied to the Oracle database used for the ARadDS from March 2021 through March 2022. Our previous reporting illustrates a pervasive issue that the Agency has in remediating information security vulnerabilities within required time frames. We made similar findings concerning the Office of Chemical Safety and Pollution Prevention's vulnerability management, as documented in OIG 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, and again in a follow-up report, Report No. 22-P-0010, *EPA Generally Adheres to Information Technology Audit Follow-Up Processes, but Management Oversight Should Be Improved*, issued December 8, 2021.

Per Section SI-2 of NIST Special Publication 800-53, Revision 5, security-relevant software and firmware updates, which include patches, must be installed within an agency-defined time frame after their release, as illustrated in Figure 3. Accordingly, the EPA's CIO 2150-P-17.2, *Information Security – Interim System and Information Integrity Procedures,* states:

> The priority of the vulnerability determines how promptly the vulnerability is implemented.
> a. Vulnerabilities ranked as "High" or "Critical" shall be mitigated and reported to CSIRC [Computer Security Incident Response Capability] within 2 calendar days (48 hours).
>
> b. Vulnerabilities ranked as "Moderate" shall be mitigated and reported to CSIRC within 7 calendar days.
>
> c. Vulnerabilities ranked as "Low" shall be mitigated and reported to CSIRC within 30 calendar days.

Figure 3: Agency vulnerability remediation time frames

Source: OIG analysis of EPA information. (EPA OIG image)

A **wide-area network** is a collection of local-area networks or other networks that communicate with one another.

OAR personnel responded that the failure to apply patches for ARadDS occurred because the system is not connected to the EPA wide-area network. This means that ARadDS would not receive automated upgrades pushed out by the Agency because its operating systems, software, and hardware were unavailable to be patched or upgraded. As a result, IT personnel must perform this process manually. OAR personnel use scanners to identify vulnerabilities and a patch manager to download and push patches to the systems. All patches must be researched, vetted carefully, and scheduled to install in conjunction with the scientists' needs to ensure successful installation. Often, the OAR stated that it runs into issues with patches due to software and hardware restrictions; the patching occurs whenever there is time, putting OAR personnel in a constant state of catch up. This resulted in the OAR's continued use of a database version that is not current in its software or hardware nor compliant in patching.

ARadDS provides historical and present information on the results of monitoring to detect radiation in air particulate, precipitation, drinking water, and surface water. Over time, these data show the fluctuations in normal background levels of environmental radiation. The data can also be used to detect higher than normal radiation levels during a radiological incident. These environmental and radiation data are used for determining responses to national incidents and safeguarding first responder personnel, but without timely patching of known vulnerabilities, the Agency risks compromising the integrity and availability of this data.

The OAR Has Not Consistently Implemented a Process for Tracking Vulnerabilities

We found that the OAR did not create POA&Ms to track remediation for the eight critical vulnerabilities assessed during our FY 2022 FISMA evaluation. Section CA-05a of NIST Special Publication 800-53 provides that a POA&M must be developed to document planned mediation actions that correct weaknesses or deficiencies. Similarly, CIO 2150-P-17.2 requires that the senior agency information security officer be notified through a POA&M via the Agency's FISMA reporting and tracking tool of any identified vulnerabilities. The OAR failed to identify these vulnerabilities in a POA&M or use the Agency's tracking tool, which serves as an information security data repository, to centrally track remediation of security weaknesses associated with information technology systems.

In response to our FY 2022 FISMA assessment documentation requests, the OAR provided ARadDS vulnerability scan results from January through May 2022. From these scan results, we identified vulnerabilities at different levels of severity, including more than 20,000 instances of critical vulnerabilities that could impact remotely operated computers on the Agency's network in various ways, such as remote code execution, denial of service, and memory corruption. The Agency was unable to provide POA&Ms to support its tracking of the remediation efforts for eight randomly selected critical vulnerabilities. The Agency attributes its failure to create POA&Ms to the significant number of vulnerabilities identified for ARadDS and the limited resources to address them. This resulted in a backlog of POA&Ms due the manual nature of the patching process and lack of an established schedule that accounts for available downtime to install these patches.

Without creating POA&Ms, the OAR is not able to strategically track and address vulnerabilities that put the confidentiality, integrity, and availability of environmental and radiation data at risk. Because of the significance of the data collected, analyzed, and hosted within ARadDS, the impact of these data being compromised poses a significant risk to public health.

Recommendations

We recommend that the assistant administrator for Air and Radiation:

2. Develop and implement a plan for prioritizing and scheduling the installation of patches that address vulnerabilities in the Analytical Radiation Data System within the time frames as set forth in CIO 2150-P-17.2, *Information Security – Interim System and Information Integrity Procedures*.

3. Assign responsibilities for the plan developed in Recommendation 2 to include documenting associated plans of actions and milestones in the Agency tracking system.

Agency Response and OIG Assessment

The OAR agreed with the OIG's findings and Recommendations 2 and 3. The OAR communicated the actions it has already taken to mitigate the risks associated with unresolved vulnerabilities such as separating the ARadDS network from the Agency's network and running its own 72-hour scans to identify security weaknesses and flaws. In response to Recommendations 2 and 3, the OAR has agreed to develop and implement a plan for prioritizing and scheduling the installation of patches, in addition to its efforts to obtain additional resources and risk acceptance from the senior information officer for those vulnerabilities that are unable to be patched within set time frames. We believe that the proposed corrective actions will satisfy the intent of the recommendations. Therefore, we consider Recommendations 2 and 3 resolved with corrective actions pending. Appendix G contains the OAR's response to the draft report.

Status of Recommendations

RECOMMENDATIONS

Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date
1	8	Update CIO 2190.0-P-01.0, *Reviewing and Updating Agencywide Directives Administered by the EPA CIO*, to include a timely process for reviewing and updating information security procedures within a year of the issuance of relevant National Institute of Standards and Technology publications.	R	Assistant Administrator for Mission Support	10/15/23
2	11	Develop and implement a plan for prioritizing and scheduling the installation of patches that address vulnerabilities in the Analytical Radiation Data System within the time frames as set forth in CIO 2150-P-17.2, *Information Security – Interim System and Information Integrity Procedures*.	R	Assistant Administrator for Air and Radiation	3/31/24
3	11	Assign responsibilities for the plan developed in Recommendation 2 to include documenting associated plans of actions and milestones in the Agency tracking system.	R	Assistant Administrator for Air and Radiation	3/31/24

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

Appendix A

Key Definitions

Analytical Radiation Data System: The OAR's nationwide environmental radiation monitoring program. It provides historical and current information on background radiation levels in the environment throughout the country. This information is used for establishing "normal" levels during cleanup of contaminated sites and when responding to suspected releases of radioactive material.

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 inspectors general 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.

Plan of Action and Milestone: A document that identifies tasks to be accomplished to address vulnerabilities. It details the resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Underlying Criteria: The 66 metrics were developed from underlying criteria consisting of OMB, 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.

Wide-Area Network: A collection of local-area networks or other networks that communicate with one another.

Appendix B

FY 2022 Core IG FISMA Metrics

The numbers in the following tables correlate to 66 total metrics of which these are the 20 core metrics for FY 2022. The source of the tables is the OMB FY 2022 Core IG Metrics implementation analysis and guidelines.

Table B-1: 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?
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 Government Furnished Equipment and Bring Your Own Device mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?
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?
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?
10. To what extent does the organization utilize technology/automation to provide a centralized, enterprisewide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?

Table B-2: Supply Chain Risk Management

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?

Table B-3: Configuration Management

20. To what extent does the organization utilize configuration settings/common secure configurations for its information systems?
21. To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities?

Table B-4: Identity, Credential, and Access Management

30. To what extent has the organization implemented strong authentication mechanisms (Personal Identity Verification or an Identity Assurance Level 3/Authenticator Assurance Level 3 credential) for nonprivileged users to access the organization's facilities (organization-defined entry/exit points), networks, and systems, including for remote access?
31. To what extent has the organization implemented strong authentication mechanisms (Personal Identity Verification or an Identity Assurance Level 3/Authenticator Assurance Level 3 credential) for privileged users to access the organization's facilities (organization-defined entry/exit points), networks, and systems, including for remote access?
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 implementing 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).

Table B-5: Data Protection and Privacy

36. To what extent has the organization implemented the following security controls to protect its Personally Identifiable Information and other agency sensitive data, as appropriate, throughout the data lifecycle—(1) encryption of data at rest, (2) encryption of data in transit, (3) limitation of transfer to removable media, and (4) sanitization of digital media prior to disposal or reuse.
37. To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses?

Table B-6: Security Training

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?

Table B-7: Information Security Continuous Monitoring

47. To what extent does the organization utilize information security continuous monitoring policies and strategies that address information security continuous monitoring requirements and activities at each organizational tier?
49. How mature are the organization's processes for performing ongoing information system assessments and granting system authorizations, including developing and maintaining system security plans, and monitoring security controls?

Table B-8: Incident Response

54. How mature are the organization's processes for incident detection and analysis?
55. How mature are the organization's processes for incident handling?

Table B-9: Contingency Planning

61. To what extent does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts?
63. To what extent does the organization perform tests/exercises of its information system contingency planning processes?

Appendix C

Information Security Reports Issued in FY 2022

The EPA OIG issued the following reports in FY 2022, which included recommendations regarding improvements within the EPA's information security program:

- Report No. 22-P-0010, *EPA Generally Adheres to Information Technology Audit Follow-Up Processes, but Management Oversight Should Be Improved*, issued December 8, 2021. We concluded that the EPA inaccurately reported its timely completion for one of 13 corrective actions related to prior cybersecurity audit recommendations and lacked management oversight to effectively resolve identified weaknesses for two of the 13 corrective actions. We found that the EPA has deficiencies in the following areas: verifying compliance with annual training requirements for information technology contractors with significant information security responsibilities; verifying corrective actions were completed as represented by the Agency; and deploying patches to mitigate identified vulnerabilities in the Agency's Pesticide Registration Information System database in a timely manner. The Agency agreed with our four recommendations; completed corrective actions for two of them; and provided acceptable planned corrective actions and estimated milestone date for the remaining two recommendations, which we considered resolved with corrective actions pending.

- Management Implication *Report*: Allowing Remote Access to Threat Actions, issued December 9, 2021. We identified a critical vulnerability concerning software installations on EPA-furnished computers. We found that the EPA had several instances of unknown third-party threat actors accessing EPA-furnished computers that would affect EPA networks, systems, and information.

- Report No. 22-E-0011, *EPA Has Not Performed Agencywide Risk Assessments, Increasing the Risk of Fraud, Waste, Abuse, and Mismanagement*, issued December 15, 2021. We concluded that the EPA had not performed agencywide entity-level risk assessments over the EPA's annual and supplemental appropriations. Specifically, the EPA had not developed or implemented an agencywide entity-level risk-assessment process in which executive officials are fully engaged in entity-level risk activities to identify high-priority risks that cut across individual Agency programs. Also, the EPA had not updated its financial management processes, policies, and procedures to identify and address risks at the agencywide entity level. As a result, the Office of the Chief Financial Officer cannot provide the direction necessary for its own office, let alone management and staff across the Agency, to perform enterprise risk-management responsibilities, including agencywide entity-level risk assessments for annual and supplemental appropriations. Without agencywide entity-level risk assessments over the EPA's annual and supplemental appropriations, the EPA cannot provide reasonable assurance that crosscutting risks are identified and mitigated and that Agency resources are directed to the most critical strategic needs. The report's two recommendations were considered resolved and the Agency completed corrective actions to address them.

- Report No. 22-P-0013, *EPA Established a Web Management Program, but Improvements Are Needed in Deploying Web Analytics*, issued December 20, 2021. We concluded that the EPA had

established a program to manage its public websites and digital services in accordance with federal laws and policies outlined in OMB M-17-06, but it had not deployed the required web analytical tracking code for 14 of the 308 public websites that provide essential environmental information to communities. This occurred because the EPA had not (1) identified a responsible office for maintaining an accurate listing of all EPA public websites and (2) established a process to validate that program offices and regions have deployed the required tracking code on all EPA public websites. Without fully implemented web analytics, the EPA could be without vital usage information to meet the needs of the public, regulatory agencies, industries, and other stakeholders when conveying environmental issues. The Agency agreed with Recommendation 1 and provided alternative language for Recommendation 2. We agreed with the Agency's suggestion and updated Recommendation 2, and consider all recommendations resolved.

- Report No. 22-E-0028, *The EPA Lacks Documented Procedures for Detecting and Removing Unapproved Software on the Agency's Network*, issued March 30, 2022. We concluded in the prior fiscal year's FISMA assessment that the EPA achieved an overall maturity level of Level 3 (Consistently Implemented) for the five security functions and the 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. The Agency agreed with our recommendations and provided acceptable planned corrective actions with estimated completion dates to address the recommendations.

OIG-Completed CyberScope Template

For Official Use Only

Inspector General Section Report	2022 IG Annual

Environmental Protection Agency

For Official Use Only

Function 0: Overall

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

Effective

Comments: The EPA has demonstrated it has consistently implemented policy, procedures, and strategies for all five of their information security function areas. The OIG assessed the five Cybersecurity Framework function areas and concluded that the EPA has achieved a Level 3, Consistently Implemented, which denotes that the Agency has consistently implemented policies, procedures, and strategies in adherence to the FY 2022 IG FISMA Reporting Metrics. While the EPA has policies, procedures, and strategies implemented for these function areas and a majority of the domains, improvements are still needed in the following areas: • Risk Management - the EPA lacks documentation of an annual review of the system security plan and implemented or inherited controls around automated tools used in risk assessments for the sampled Analytical Radiation Data System. • Configuration Management - For the sampled Analytical Radiation Data System, we found the Agency did not: o Create plans of action and milestones to track the remediation of a sample of eight randomly selected critical vulnerabilities within two days as required by the Agency's Chief Information Officer Directive 2150-P-17.2, Information Security - Interim System and Information Integrity Procedures. o With respect to FY Core IG Metrics Question 21, apply patches to remediate vulnerabilities in a timely manner as required by Directive 2150-P-17.2.

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.

The EPA has demonstrated it has consistently implemented policy, procedures, and strategies for all five of their information security function areas. The Office of Inspector General assessed the five Cybersecurity Framework function areas and concluded that the EPA has achieved a Level 3, Consistently Implemented, which denotes that the Agency has consistently implemented policies, procedures, and strategies in adherence to the FY 2022 Inspector General Federal Information Security Modernization Act, or FISMA, Reporting Metrics. While the EPA has policies, procedures, and strategies implemented for these function areas and a majority of the domains, improvements are still needed in the following areas: • Risk Management - the EPA lacks documentation of an annual review of the system security plan and implemented or inherited controls around automated tools used in risk assessments for the sampled Analytical Radiation Data System. • Configuration Management - For the sampled Analytical Radiation Data System, we found the Agency did not: o Create plans of action and milestones to track the remediation of a sample of eight randomly selected critical vulnerabilities within two days as required by the Agency's Chief

Function 0: Overall

Information Officer Directive 2150-P-17.2, Information Security - Interim System and Information Integrity Procedures. o With respect to FY Core IG Metrics Question 21, apply patches to remediate vulnerabilities in a timely manner as required by Directive 2150-P-17.2.

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. 5: CA-3 and PM-5; NIST Cybersecurity Framework (CSF): ID.AM-1 - 4; FY 2022 CIO FISMA Metrics: 1.1-1.1.5, 1.3; OMB A-130, NIST SP 800-37, Rev. 2: Task P-18; NIST 800-207, Section 7.3; EO 14028, Section 3; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B and D (5); CISA Cybersecurity & Incident Response Playbooks)

   Ad Hoc (Level 1)

   Comments: This rating remains unchanged from the previous year's rating because corrective actions to address FY 2021 findings related to this metric are not planned to be implemented until completion dates of October 31, 2022 and January 31, 2023.

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. 5: CA-7 and CM-8; NIST SP 800-137; NIST IR 8011; NIST 800-207, 7.3.2; Federal Enterprise Architecture (FEA) Framework, v2; FY 2022 CIO FISMA Metrics: 1.2-1.2.3; CSF: ID.AM-1, ID.AM-5; NIST SP 800-37, Rev. 2: Task P-10 and P-16; NIST 800-207, Section 7.3; EO 14028, Section 3; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8: Control 1)

   Consistently Implemented (Level 3)

   Comments: See remarks in question 11.1.

3. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of software 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. 5: CA-7, CM-8, CM-10, and CM-11; NIST SP 800-137; NIST IR 8011; FEA Framework, v2; FY 2022 CIO FISMA Metrics: 1.3 and 4.0; OMB M-21-30; EO 14028, Section 4; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B; CSF: ID.AM-2; NIST SP 800- 37, Rev. 2: Task P-10 and P-16; NIST 800-207, Section 7.3; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8: Control 2)

   Ad Hoc (Level 1)

   Comments: This rating remains unchanged from the previous year's rating because corrective actions to address FY 2021 findings related to this metric are not planned to be implemented until completion dates of October 31, 2022 and January 31, 2023.

Function 1A: Identify - Risk Management

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 2022 CIO FISMA Metrics: 1.1; OMB M-19-03; NIST SP 800-37, Rev. 2: Task C-2, C-3, P-12, P-13, S-1 - S-3)?

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. 5: RA-3 and 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 P2, P-3, P-14, R-2, and R-3)

Consistently Implemented (Level 3)

Comments: See remarks in question 11.1.

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 800-161; NIST SP 800-163, Rev. 1 CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

7. To what extent have roles and responsibilities of internal and external stakeholders involved in cyber security risk management processes been defined and communicated 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; NISTIR 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)?

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-19-03, CSF v1.1, ID.RA-6)?

9. To what extent does the organization ensure that information about cyber security risks is communicated in a timely manner to all necessary internal and external stakeholders (OMB A-123; OMB Circular A-11; Green Book (Principles #9, #14 and #15); OMB M-19-03; CSF: Section 3.3; NIST SP 800-37 (Rev. 2) Task M-5; SECURE Technology Act: s. 1326, NISTIR 8286)?

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; NIST IR 8286; CISA Zero Trust Maturity Model, Pillars 2-4, NIST 800-207, Tenets 5 and 7; OMB M-22-09, Federal Zero Trust Strategy, Security Orchestration, Automation, and Response)

Consistently Implemented (Level 3)

Function 1A: Identify - Risk Management

Comments: See remarks in question 11.1.

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

Consistently Implemented (Level 3)

Comments: We determined that overall maturity of Risk Management was Level 3, Consistently Implemented, based on the majority of FY 2022 Core IG FISMA Metrics in the Risk Management domain being rated at Level 3, Consistently Implemented.

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?

Function 1B: Identify - Supply Chain Risk Management

12. To what extent does the organization utilize supply chain risk management policies and procedures to manage SCRM activities at all organizational tiers (NIST SP 800-37 Rev. 2, Section 2.8, NIST 800-53, SR-1, NIST CSF v1.1, ID.SC-1, NIST 800-161)?

13. To what extent does the organization utilize a supply chain risk management plan(s) to ensure the integrity, security, resilience, and quality of services, system components, and systems (OMB A-130, NIST SP 800-37 Rev. 2, Section 2.8, NIST 800-53, SR-2, SR-3; NIST 800-161, section 2.2.4 and Appendix E)?

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 and 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, NIST 800-218, Task PO.1.3; FY 2022 CIO FISMA Metrics: 7.4.2; CIS Top 18 Security Controls v.8: Control 15)

Consistently Implemented (Level 3)

Comments: See remarks in question 16.1.

15. To what extent does the organization maintain and monitor the provenance and logistical information of the systems and system components it acquires? (NIST SP 800-53 REV. 5: SR-4 and NIST SP 800-161, Provenance (PV) family)?

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

Consistently Implemented (Level 3)

Comments: We determined that overall maturity of Supply Chain Risk Management was Level 3, Consistently Implemented, based on FY 2022 Core IG Metrics question 14 being rated at Level 3, Consistently Implemented.

Function 1B: Identify - Supply Chain Risk Management

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

Consistently Implemented (Level 3)

Comments: Auditors determined that because the overall maturity ratings of the Risk Management domain and Supply Chain Management domain were both Level 3, Consistently Implemented, the majority of the FY 2022 Core IG Metrics for the Identify function are rated at Level 3, Consistently Implemented.

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?

Function 2A: Protect - Configuration Management

17. To what extent 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)?

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)?

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 2022 CIO FISMA Metrics: 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1)?

20. To what extent does the organization utilize settings/common secure configurations for its information systems? (NIST SP 800-53, Rev. 5: CM-6, CM-7, and RA-5; NIST SP 800-70, Rev. 4; FY 2022 CIO FISMA Metrics, Section 7, Ground Truth Testing; EO 14028, Section 4, 6, and 7; OMB M-22-09, Federal Zero Trust Strategy, Section D; OMB M - 22-05; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8, Controls 4 and 7; CSF: ID.RA-1 and DE.CM-8)

Defined (Level 2)

Comments: We found the Agency did not have plans of action and milestones to track the remediation of a sample of eight randomly selected critical vulnerabilities for the sampled Analytical Radiation Data System within two days as required by the Agency's information security procedures.

21. To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities? (EO 14028, Sections 3 and 4; NIST SP 800-53, Rev. 5: CM-3, RA-5, SI-2, and SI-3; NIST SP 800-40, Rev. 3; NIST 800-207, section 2.1; CIS Top 18 Security Controls v.8, Controls 4 and 7; FY 2022 CIO FISMA Metrics: Section 8; CSF: ID.RA-1;

Function 2A: Protect - Configuration Management

DHS Binding Operational Directives (BOD) 18-02, 19-02, and 22-01; OMB M-22-09, Federal Zero Trust Strategy, Section D; CISA Cybersecurity Incident and Vulnerability Response Playbooks)

Defined (Level 2)

Comments: We found the Agency has not applied patches to remediate vulnerabilities for the sampled Analytical Radiation Data System in a timely manner as required by the Agency's patch management procedures.

22. To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-19-26)?

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).

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)?

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

Defined (Level 2)

Comments: We determined that overall maturity of Configuration Management was Level 2, Defined, based on all FY 2022 Core IG Metrics in the Configuration Management domain being rated at Level 2, Defined.

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?

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 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 Roadmap and Implementation Guidance (FICAM), OMB M-19-17)?

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

Function 2B: Protect - Identity and Access Management

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

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)?

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 nonprivileged users to access the organization's facilities [organizationdefined entry/exit points], networks, and systems, including for remote access? (EO 14028, Section 3; HSPD-12; NIST SP 800-53, Rev. 5: 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 2022 CIO FISMA Metrics: Section 2; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section A (2); CSF: PR.AC-1 and 6; OMB M19-17, NIST SP 800-157; NIST 800-207 Tenet 6; CIS Top 18 Security Controls v.8: Control 6)

Consistently Implemented (Level 3)

Comments: See remarks in question 34.1.

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? (EO 14028, Section 3; HSPD-12; NIST SP 800-53, Rev. 5: AC-17 and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63 and 800-157; OMB M-19-17; FY 2022 CIO FISMA Metrics: Section 2; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section A (2); CSF: PR.AC-1 and 6; DHS ED 19-01; NIST 800-207 Tenet 6; CIS Top 18 Security Controls v.8: Control 6)

Consistently Implemented (Level 3)

Comments: See remarks in question 34.1.

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? (EO 14028, Section 8; FY 2022 CIO FISMA Metrics: 3.1; OMB M-21-31; OMB M-19-17; NIST SP 800-53, Rev. 5: AC-1, AC2, AC-5, AC-6, AC-17; AU-2, AU-3, AU-6, and IA-4; DHS ED 19-01; CSF: PR.AC-4; CIS Top 18 Security Controls v.8: Controls 5, 6, and 8)

Consistently Implemented (Level 3)

Comments: See remarks in question 34.1.

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 2022 CIO FISMA Metrics: 2.10 and 2.11).

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

Consistently Implemented (Level 3)

Comments: We determined that the overall maturity of Identity and Access Management was Level 3, Consistently Implemented, based on all FY 2022 Core IG Metrics for the Identity and Access Management domain being rated at Level 3, Consistently Implemented.

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?

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))?

36. To what extent has the organization implemented the encryption of data rest, in transit, limitation of transference of data by removable media, and sanitization of digital media prior to disposal or reuse to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? (EO 14028, Section 3(d); OMB M-22-09, Federal Zero Trust Strategy; NIST 800-207; NIST SP 800-53, Rev. 5; SC-8, SC28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2022 CIO FISMA Metrics: 2.1, 2.2, 2.12, 2.13; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6; CIS Top 18 Security Controls v. 8: Control 3)

Consistently Implemented (Level 3)

Comments: See remarks in question 40.1.

37. To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (FY 2022 CIO FISMA Metrics, 5.1; NIST SP 800-53, Rev. 5: SI3, SI-7, SI-4, SC-7, and SC-18; DHS BOD 18-01; DHS ED 19- 01; CSF: PR.DS-5, OMB M-21-07; CIS Top 18 Security Controls v.8: Controls 9 and 10)

Consistently Implemented (Level 3)

Comments: See remarks in question 40.1.

Function 2C: Protect - Data Protection and Privacy

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)?

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)

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

Consistently Implemented (Level 3)

Comments: We determined that the overall maturity of Data Protection and Privacy was Level 3, Consistently Implemented, based on all FY 2022 Core IG Metrics for the Data Protection and Privacy domain being rated at Level 3, Consistently Implemented.

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?

Function 2D: Protect - Security Training

41. To what extent 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).

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? (FY 2022 CIO FISMA Metrics, Section 6; NIST SP 800-53, Rev. 5: AT-2, AT-3, and PM-13; 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 Top 18 Security Controls v.8: Control 14)

Consistently Implemented (Level 3)

Comments: See remarks in question 46.1.

43. 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

Function 2D: Protect - Security Training

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).

44. To what extent 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 2022 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4).

45. To what extent 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 2022 CIO FISMA Metrics: 2.15)?

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

Consistently Implemented (Level 3)

Comments: We determined that the overall maturity of Security Training was Level 3, Consistently Implemented, based on all FY 2022 Core IG Metrics for the Security Training domain being rated at Level 3, Consistently Implemented.

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

Consistently Implemented (Level 3)

Comments: Auditors determined that despite the Configuration Management domain being rated at Level 2, Defined, because the overall maturity of Identity and Access Management was Level 3, Consistently Implemented, and the overall maturity of the Data Protection and Privacy domain was Level 3, Consistently Implemented, a simple majority of the FY 2022 Core IG Metrics for the Protect function are rated at Level 3, Consistently Implemented.

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?

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 800-53, Rev. 5: CA-7, PM-6, PM-14, and PM-31; NIST SP 800-37 (Rev. 2) Task P-7; NIST SP 800-137: Sections 3.1 and 3.6; CIS Top 18 Security Controls v.8: Control 13)

Consistently Implemented (Level 3)

Comments: While auditors assessed this metric at Level 3, Consistently Implemented, we recommend the Agency capture

Function 3: Detect - ISCM

lessons learned in its Continuous Monitoring Plans as it matures its ISCM practices.

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; NIST 800-37, Rev. 2 Task P-7 and S-5)

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. 5: CA-2, CA-5, CA-6, CA-7, PL-2, and PM-10; NIST Supplemental Guidance on Ongoing 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 51.1.

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

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

Consistently Implemented (Level 3)

Comments: We determined that the overall maturity of ISCM was Level 3, Consistently Implemented, based on all FY 2022 Core IG Metrics in the ISCM domain being rated at Level 3, Consistently Implemented.

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?

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)?

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; CSF, RS.CO-1, OMB M-20-04; FY 2022 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?

54. How mature are the organization's processes for incident detection and analysis? (EO 14028, Section 6; OMB M-22-05, Section I;

Function 4: Respond - Incident Response

CISA Cybersecurity Incident and Vulnerability Response Playbooks; FY 2022 CIO FISMA Metrics: 10.6; NIST 800-53, Rev. 5: IR-4, IR-5, and IR-6; NIST SP 800-61 Rev. 2; OMB M20-04; CSF: DE.AE-1, DE.AE-2 -5, PR.DS-6, RS.AN-1 and 4, and PR.DS-8; and CIS Top 18 Security Controls v.8: Control 17)

Consistently Implemented (Level 3)

Comments: See remarks in question 59.1.

55. How mature are the organization's processes for incident handling? (EO 14028, Section 6; OMB M-22-05, Section I; CISA Cybersecurity Incident and Vulnerability Response Playbooks; FY 2022 CIO FISMA Metrics: 10.6; NIST 800-53, Rev. 5: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2)

Consistently Implemented (Level 3)

Comments: See remarks in question 59.1.

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)

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).

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

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

Consistently Implemented (Level 3)

Comments: We determined that the overall maturity of Incident Response was Level 3, Consistently Implemented, based on all FY 2022 Core IG Metrics in the Incident Response domain being rated at Level 3, Consistently Implemented.

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?

Function 5: Recover - Contingency Planning

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, CP-2, and CP-3; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?

61. To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts? (FY 2022 CIO FISMA Metrics: 10.1.4; NIST SP 800-53, Rev. 5: CP-2, and RA-9; NIST SP 800-34, Rev. 1, 3.2; NIST IR 8286; FIPS 199; FCD-1; OMB M-19-03; CSF:ID.RA-4)

Consistently Implemented (Level 3)

Comments: See remarks in question 66.1.

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 2022 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?

63. To what extent does the organization perform tests/exercises of its information system contingency planning processes? (FY 2022 CIO FISMA Metrics: 10.1; NIST SP 800-34; NIST SP 800-53, Rev. 5: CP-3 and CP-4; CSF: ID.SC-5 and CSF: PR.IP10; CIS Top 18 Security Controls v.8: Control 11)

Consistently Implemented (Level 3)

Comments: See remarks in question 66.1.

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 2022 CIO FISMA Metrics, Section 5; and NARA guidance on information systems security records)?

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)?

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

Consistently Implemented (Level 3)

Comments: We determined that the overall maturity of the Recover function and Contingency Planning domain was Level 3, Consistently Implemented, based on the FY 2022 Core IG Metrics in the Contingency Planning domain being rated at Level 3, Consistently Implemented.

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?

APPENDIX A: Maturity Model Scoring

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

Summary

Cycle	Maturity Level	Mean	Mode
FY22 Core Metrics	Consistently Implemented (Level 3)	2.78	Consistently Implemented (Level 3)
FY22 Supplementary Metrics			
FY22 Overall	Consistently Implemented (Level 3)	2.78	Consistently Implemented (Level 3)

Overall

Function	Calculated Maturity Level	Mean	Mode	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management / Supply Chain Risk Management	Consistently Implemented (Level 3)	2.33	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Auditors determined that because the overall maturity ratings of the Risk Management domain and Supply Chain Management domain were both Level 3, Consistently Implemented, the majority of the FY 2022 Core IG Metrics for the Identify function are rated at Level 3, Consistently Implemented.

APPENDIX A: Maturity Model Scoring

Function 2: Protect - Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	Consistently Implemented (Level 3)	2.82	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Auditors determined that despite the Configuration Management domain being rated at Level 2, Defined, because the overall maturity of Identity and Access Management was Level 3, Consistently Implemented, and the overall maturity of the Data Protection and Privacy domain was Level 3, Consistently Implemented, a simple majority of the FY 2022 Core IG Metrics for the Protect function are rated at Level 3, Consistently Implemented.
Function 3: Detect - ISCM	Consistently Implemented (Level 3)	3.00	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that the overall maturity of ISCM was Level 3, Consistently Implemented, based on all FY 2022 Core IG Metrics in the ISCM domain being rated at Level 3, Consistently Implemented.
Function 4: Respond - Incident Response	Consistently Implemented (Level 3)	3.33	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that the overall maturity of Incident Response was Level 3, Consistently Implemented, based on all FY 2022 Core IG Metrics in the Incident Response domain being rated at Level 3, Consistently Implemented.

APPENDIX A: Maturity Model Scoring

Function 5: Recover - Contingency Planning	Consistently Implemented (Level 3)	3.33	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that the overall maturity of the Recover function and Contingency Planning domain was Level 3, Consistently Implemented, based on the FY 2022 Core IG Metrics in the Contingency Planning domain being rated at Level 3, Consistently Implemented.
Function 0: Overall	Not Effective	2.78	Consistently Implemented (Level 3)	Effective	The EPA has demonstrated it has consistently implemented policy, procedures, and strategies for all five of their information security function areas. The OIG assessed the five Cybersecurity Framework function areas and concluded that the EPA has achieved a Level 3, Consistently Implemented, which denotes that the Agency has consistently implemented policies, procedures, and strategies in adherence to the FY 2022 IG FISMA Reporting Metrics. While the EPA has policies, procedures, and strategies

Function 4: Respond - Incident Response

Function	Count
Ad Hoc (Level 1)	0

APPENDIX A: Maturity Model Scoring

Defined (Level 2)	0
Consistently Implemented (Level 3)	0
Managed and Measurable (Level 4)	0
Optimized (Level 5)	0
Ad Hoc (Level 1)	0
Defined (Level 2)	0
Consistently Implemented (Level 3)	0
Managed and Measurable (Level 4)	0
Optimized (Level 5)	0
Ad Hoc (Level 1)	0
Defined (Level 2)	0
Consistently Implemented (Level 3)	0
Managed and Measurable (Level 4)	0
Optimized (Level 5)	0
Ad Hoc (Level 1)	0
Defined (Level 2)	0
Consistently Implemented (Level 3)	0
Managed and Measurable (Level 4)	0
Optimized (Level 5)	0
Ad Hoc (Level 1)	0

APPENDIX A: Maturity Model Scoring

Defined (Level 2)	0
Consistently Implemented (Level 3)	0
Managed and Measurable (Level 4)	0
Optimized (Level 5)	0
Ad Hoc (Level 1)	0
Defined (Level 2)	0
Consistently Implemented (Level 3)	0
Managed and Measurable (Level 4)	0
Optimized (Level 5)	0
Ad Hoc (Level 1)	0
Defined (Level 2)	0
Consistently Implemented (Level 3)	0
Managed and Measurable (Level 4)	0
Optimized (Level 5)	0
Ad Hoc (Level 1)	0
Defined (Level 2)	0
Consistently Implemented (Level 3)	0
Managed and Measurable (Level 4)	0
Optimized (Level 5)	0
Ad Hoc (Level 1)	0

APPENDIX A: Maturity Model Scoring

Defined (Level 2)	0
Consistently Implemented (Level 3)	0
Managed and Measurable (Level 4)	0
Optimized (Level 5)	0

Appendix E

EPA FY 2022 FISMA Compliance Results

Table E-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 3: Consistently Implemented
Protect	Configuration Management	Level 2: Defined
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

Source: OIG assessment results. (EPA OIG table)

The EPA's overall maturity rating is Level 3 (Consistently Implemented).

The OMS's Response to Draft Report

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

OFFICE OF MISSION SUPPORT

MEMORANDUM

SUBJECT: Response to Office of Inspector General Draft Report No. OA-FY22-0134 "*The EPA's Processes for Tracking and Remediating Vulnerabilities and Reviewing Information Technology Procedures Are Implemented Inconsistently*," dated April 6, 2023

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

VAUGHN NOGA Digitally signed by VAUGHN NOGA Date: 2023.05.17 09:06:46 -04'00'

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

Thank you for the opportunity to respond to the subject audit report. The following summarizes the Office of Mission Support's (OMS) overall position, along with its position on the report recommendation that was direct to us.

AGENCY'S RESPONSE TO DRAFT AUDIT RECOMMENDATIONS

Disagreement

OMS agrees with the OIG's findings or the intention of its recommendation. We have begun to develop programmatic changes which will address the concerns of the Office of Inspector General. As it is currently written, however, the recommendation may not be achievable within the given timeframe. We request your consideration of our explanation and proposed recommendation, which we believe fully addresses the intention of the original recommendation.

No.	Recommendation	Assigned to:	Agency Response	Proposed Alternative
1	Update CIO 2190.0-P-01.0, *Reviewing and Updating Agencywide Directives Administered by the EPA CIO,* to include a timely process for reviewing and updating information security procedures within a year of the issuance of relevant National Institute of Standards and Technology publications.	OMS OCAPPM	The recommendation to update our review policy within a year of NIST publications is too narrow. We would recommend amending our policy to be broader of external factors that would necessitate a sooner or different time requirement to review and update our CIO policies, such as, congressional acts, executive orders, NIST publications, and other federal mandates and guidance.	Update CIO 2190.0-P-01.0, *Reviewing and Updating Agencywide Directives Administered by the EPA CIO*, to include exceptions of federal mandates and guidance, such as, National Institute of Standards and Technology (NIST) publications, which require a timely process for reviewing and updating CIO policies within a year of the issuance of relevant NIST publications. Proposed Completion Date: October 15, 2023

Attachment:

CC: LaVonda Harris-Claggett
Eric Jackson Jr.
Alonzo Munyeneh
Jeremy Sigel
Sabrena Stewart
Erin Collard
David Alvarado
Austin Henderson
Kristi Wells
Gary Farley

Beth Jones
Holly Fenderson
Tonya Manning
Mark Bacharach
Lee Kelly
Dan Coogan
Jan Jablonski
Marilyn Armstrong
OMS_Audit_Coordination@epa.gov
Grant Peacock
Susan Perkins
Andrew LeBlanc

The OAR's Response to Draft Report

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

OFFICE OF
AIR AND RADIATION

May 5, 2023

MEMORANDUM

SUBJECT: EPA Response to OIG Draft Report titled: "FY22 EPA FISMA, The EPA's Processes for Tracking and Remediating Vulnerabilities and Reviewing Information Technology Procedures Are Implemented Inconsistently. Project No. OA-FY22- 0134, April 6, 2023

FROM: Joseph Goffman
Principal Deputy Assistant Administrator
Office of Air and Radiation

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

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG's) draft report titled, "*The EPA's Processes for Tracking and Remediating Vulnerabilities and Reviewing Information Technology Procedures Are Implemented Inconsistently,*" Project No. OA-FY22- 0134, April 6, 2023. The Office of Air and Radiation (OAR) is responding to Recommendations 2 and 3 in the report which relate to the Analytical Radiation Data System (ARadDS) operated by the National Analytical Radiation Environmental Laboratory (NAREL), which is part of OAR's Office of Radiation and Indoor Air.

OAR agrees that persistent vulnerability mitigation and remediation is critical to maintaining a strong cybersecurity posture and requires priority attention. Not doing so may leave vulnerable platforms susceptible to cybersecurity threats and attacks and we support implementation of security measures that reduce such risks.

OAR also agrees in principle with the findings and Recommendations 2 and 3 of the draft report., however, for the reasons explained below, is somewhat constrained in our ability to fully implement the Recommendations.

Recommendation 2: "Develop and implement a plan for prioritizing and scheduling the installation of patches that address vulnerabilities in the Analytical Radiation Data System within the time frames as set forth in CIO 2150-P-17.2, Information Security – Interim System and Information Integrity Procedures."

Response to Recommendation 2:

For systems that can be patched, the OAR will develop and implement a plan for prioritizing and scheduling the installation of patches that address vulnerabilities in the ARadDS (Analytical Radiation Data System) generally within the time frames set forth in CIO 2150-P-17.2, Information Security – Interim System and Information Integrity Procedures.

The ARadDS supports and maintains three unique national assets that provide the primary source of data to all government agencies via EPA's RadNet Program (High Value Asset), the fixed National Analytical Radiation Environmental Laboratory (NAREL), and the Mobile Environmental Radiation Laboratory (MERL). The RadNet, NAREL fixed laboratory, and MERL are three of the EPA's five Critical Infrastructure and Key Resources (CI/KR).

Nuclear counting instruments that measure radiation data and support these assets are not regularly updated by manufacturers. This results in outdated hardware and software that is not able to be patched because doing so breaks the systems or dependent systems. Such breakdowns can result in the inability to provide critical national radiation monitoring data to EPA and the public. Therefore, rigorous testing is done on available patches; it can often take several months to implement patches that will not interfere with our ability to perform our mission.

Notwithstanding the limitations of older counting equipment, compounded by resource limitations, efforts to mitigate the issues caused by the inability to remediate vulnerabilities immediately have been put into action.

Actions Implemented:

- Separation of the ARadDS network from the EPA WAN so that vulnerabilities that exist do not put the entire agency's network at risk.
- Demilitarized Zone (DMZ) implementation to assist with network segmentation of possible vulnerable laboratory systems.
- FY23 - Installed and configured Windows 10 Enterprise Long-Term Servicing Channel (LTSC) on instrument-dependent systems that require less updating and a 10-year lifecycle, guaranteeing features, functionality, and support.
- Vulnerability scans conducted on the ARadDS network every 72-hours to identify security weaknesses and flaws. The scans are submitted weekly to the Office of Mission Support (OMS) ticketing system to be uploaded into the agency's vulnerability scanning platform instance for transparency.

- The ARadDS utilizes security information and event management (SIEM) software for continuous monitoring of the network to detect, identify, and prevent threats.
- Isolation of the laboratory environment and systems that have limited access, implementation of muti-factor authentication, and the requirement of laboratory personnel to be on premise to utilize systems.

Actions In Progress:

- FY23 - OAR funded 2 new cybersecurity positions for additional support in monitoring, mitigating, and remediating vulnerabilities and strengthening the ARadDS security posture. This IT support contract is awaiting award.
- FY23 - OAR funded hardware solutions to replace outdated storage, servers, and switches. This also included a high availability firewall design that will assist with internal network segmentation and protection, furthering vulnerability mitigation.
- FY23 - Seeking $2.5M from the Technology Modernization Fund (TMF) to assist with additional modernization in outdated hardware and software across the ARadDS network to prepare for the possible future migration to the cloud. If awarded this will:
    - Add 2 IT contractor personnel for a guaranteed 3 years;
    - Hardware & software modernization (virtualization, acquire automated cybersecurity tools, virtual private network solution (VPN); and
    - Antiquated laboratory information management system (LIMS) replacement.
- The President's Budget Request for FY24 includes an increase to update the aging equipment that monitors the nation's air for radiation. This also will support and modernize the IT infrastructure for ARaDS and support enhanced lab and field office facility operations and maintenance. (See p.119 of the United States Environmental Protection Agency Fiscal Year 2024 Justification of Appropriation Estimates for the Committee on Appropriations.)

In addition to the mitigation efforts above, the ARadDS network seeks risk acceptance from the OAR Senior Information Official (SIO) annually for the vulnerabilities that are unable to be patched within set timelines.

Planned Completion Date: Fiscal Year (FY) 2024, Quarter (Q) 2 - plan for prioritizing and scheduling the installation of patches.

Recommendation 3: "Assign responsibilities for the plan developed in Recommendation 2 to include documenting associated plans of actions and milestones in the Agency tracking system."

Response to Recommendation 3: The OAR will assign responsibility for the plan

developed in Recommendation 2, the NAREL laboratory director who is the ARadDS System Owner, The ARadDS network is supported by five contractor personnel, one of whom (the system administrator), is responsible for supporting the entirety of the ARadDS network. At present, these personnel are fully occupied maintaining full functionality and up time of the current system and meeting those requirements. There is no additional bandwidth to take on the submission of thousands of Plans of Action and Milestones (POA&Ms) for vulnerabilities that are not remediated within the timeframes set forth in CIO 2150-P-17.2, Information Security – Interim System and Information Integrity Procedures. Even with the addition of two more contractor personnel, who will be taking on cybersecurity duties, NAREL will be unable to document associated POA&Ms in the agency's tracking system for vulnerabilities that are not remediated. In addition, for those vulnerabilities that have do have POA&Ms in the agency's tracking system, there is currently no process within the EPA that allows for automated comparison of new or existing vulnerabilities, thereby making the tracking and resolution of vulnerabilities essentially a labor-intensive manual process.

The ARadDS network seeks risk acceptance from the OAR Senior Information Official (SIO)

annually for the submission of POA&Ms for each vulnerability that is not remediated. The POA&Ms are entered into the agency's tracking system (Xacta) and reviewed annually to see if alternate methods have become available to implement fixes that better meet agency expectations.

Planned Completion Date: Fiscal Year (FY) 2024, Quarter (Q) 2

Appendix H

Distribution

The Administrator
Deputy Administrator
Chief of Staff, Office of the Administrator
Deputy Chief of Staff for Management, Office of the Administrator
Assistant Administrator for Mission Support
Assistant Administrator for Air and Radiation
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 Air and Radiation
Deputy Assistant Administrator for Stationary Sources, Office of Air and Radiation
Deputy Assistant Administrator for Mobile Sources, Office of Air and Radiation
Deputy Assistant Administrator for Air and Radiation
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, 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
Audit Follow-Up Coordinator, Office of Air and Radiation

Whistleblower Protection

U.S. Environmental Protection Agency

The Whistleblower Protection Coordinator's role is to educate Agency employees about prohibitions on retaliation and employees' rights and remedies in cases of reprisal. For more information, please visit the Whistleblower Protection Coordinator's webpage.

Contact us:

Congressional Inquiries: OIG.CongressionalAffairs@epa.gov

Media Inquiries: OIG.PublicAffairs@epa.gov

EPA OIG Hotline: OIG_Hotline@epa.gov

Web: epa.gov/oig

Follow us:

Twitter: @epaoig

LinkedIn: linkedin.com/company/epa-oig

YouTube: youtube.com/epaoig

Instagram: @epa.ig.on.ig