OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

February 1, 2024

MEMORANDUM

SUBJECT: Notification:
Audit of the EPA’s Compliance with the Federal Information Security Modernization Act for Fiscal Year 2024
Project No. OA-FY24-0045

FROM: LaSharn Barnes, Director
LASHARN BARNES
Digitally signed by LASHARN BARNES
Date: 2024.01.31 15:18:40 -05'00'
Information Resources Management Directorate
Office of Audit

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

The U.S. Environmental Protection Agency Office of Inspector General plans to begin an audit of the EPA’s compliance with the Federal Information Security Modernization Act of 2014, or FISMA. This audit is statutorily required and is part of the OIG’s oversight plan for fiscal year 2024.

Our objective is to assess the EPA’s compliance with the Office of Management and Budget’s *FY 2023–2024 Inspector General Federal Information Security Modernization Act (FISMA) Reporting Metrics,* dated February 10, 2023. We plan to conduct work within the Office of Mission Support at EPA headquarters. We will use applicable generally accepted government auditing standards to conduct our audit. The anticipated benefit of this audit is the fulfilment of a congressional mandate to assess the Agency’s information security program against FY 2024 FISMA requirements.

We will contact you to arrange a mutually agreeable time to discuss our objective. At that time, we can discuss any concerns that you may have and answer any questions about the audit process, reporting procedures, methods used to gather and analyze data, and what we should expect of each other during the audit. Throughout the audit, we will provide updates on a regular basis.

To expedite our audit, please be ready to provide the information we have requested in Appendix A within three days of the entrance conference or as soon as possible after receipt of this notification memorandum. This information relates to the EPA’s information technology processes and its enterprise wide area network.

We respectfully note that the Inspector General Act of 1978, as amended, authorizes the OIG to have timely access to personnel and all materials necessary to complete our objective. Similarly, EPA Manual 6500, *Functions and Activities of the Office of Inspector General* (1994), requires that each EPA employee cooperate with and fully disclose information to the OIG. Also, Administrator Michael S. Regan, in a

May 16, 2023 email to EPA employees, stated that the "agency and its employees have a duty to cooperate with OIG" and observed that "full engagement and collaboration between the OIG and EPA provides our agency with the opportunity to improve program performance and efficiency." If an Agency employee or contractor refuses to provide requested materials to the OIG or otherwise fails to cooperate with the OIG, we will request that you immediately resolve the situation. Consistent with the Inspector General Act, we may report unresolved access matters to the administrator and to Congress.

We will post this memorandum on our public website at www.epaoig.gov. Anyone with knowledge of potential fraud, waste, abuse, misconduct, or mismanagement related to this audit should contact the OIG Hotline at (888) 546-8740 or via an electronic form on the "OIG Hotline" webpage.

Attachment

cc: Janet McCabe, Deputy Administrator
Dan Utech, Chief of Staff, Office of the Administrator
Wesley J. Carpenter, Deputy Chief of Staff for Management, Office of the Administrator
Vaughn Noga, Chief Information Officer and Deputy Assistant Administrator for Information Technology and Information Management, Office of Mission Support
Helena Wooden-Aguilar, Deputy Assistant Administrator for Workforce Solutions and Inclusive Excellence, Office of Mission Support
Dan Coogan, Deputy Assistant Administrator for Infrastructure and Extramural Resources, Office of Mission Support
Yulia Kalikhman, Acting Director, Office of Resources and Business Operations, Office of Mission Support
Tonya Manning, Director and Chief Information Security Officer, Office of Information Security and Privacy, Office of Mission Support
Afreeka Wilson, Audit Follow-Up Coordinator, Office of Mission Support
Susan Perkins, Agency Follow-Up Coordinator
Andrew LeBlanc, Agency Follow-Up Coordinator
José Kercado, Agency Follow-Up Coordinator
Nick Conger, Associate Administrator for Public Affairs
Terrance Jackson, Acting Director, Office of Administrative and Executive Services, Office of the Administrator
Audit Follow-Up Coordinators
Sean W. O'Donnell, Inspector General
Nicole N. Murley, Deputy Inspector General

APPENDIX A: Information and Process Walk-Through Requests

Note: We have provided tables detailing the related FISMA metrics in Appendix B.

Table A-1: Information requests

Related FISMA metric number	OIG request number	Request	Agency response
4	**1**	What Agency information technology procedures detail the extent to which the EPA categorizes and communicates the importance and priority of information systems in enabling its mission and business functions, including for high value assets? The OIG has reviewed the following procedures and did not identify this information: ○ CIO 2150-P-23.2, *Information Security–Program Management (PM) Procedure*, dated December 2023. ○ CIO 2150-P-14.3, *Information Security–Risk Assessment (RA) Procedure*, dated December 2023. If we overlooked it, please provide the specific sections of the procedures in which this information is located.	
6	**2**	What Agency information technology procedures detail the EPA's software assurance processes for mobile applications? The OIG has reviewed the following procedures and did not identify this information: ○ CIO 2150.3-P-12.2, *Information Security–Planning (PL) Procedure*, dated December 2023. ○ CIO 2150.3-P-15.2, *Information Security–System and Service Acquisition (SA) Procedures*, dated December 2023. ○ CIO 2150-P-23.2, *Information Security–Program Management (PM) Procedure*, dated December 2023. ○ CIO 2150-P-26.0, *Information Security–Supply Chain Risk Management (SR) Procedure*, dated November 2023. If we overlooked it, please provide the specific sections of the procedures in which this information is located.	
38	**3**	What is the most up-to-date version of CIO 2151-P-02.4, *Responding to Personally Identifiable Information (PII) Breach Procedure*, that the EPA is using for the *Data Breach Response Plan*?	

Related FISMA metric number	OIG request number	Request	Agency response
42	**4**	Please provide the FY 2023 Information Security and Privacy Training report.	
50	**5**	What Agency information technology procedures define the format of reports and the tools used to provide performance measurements and control risk evaluation to individuals with significant security responsibilities. The OIG has reviewed the following procedures and did not identify this information: ○ CIO 2150-P-04.3, *Information Security–Assessment, Authorization and Monitoring (CA) Procedure,* dated June 2023. ○ *Information Security Continuous Monitoring Strategic Plan FY 2015*, dated April 17, 2015. If we overlooked it, please provide the specific sections of the procedures in which this information is located.	
All	**6**	Have there been any major information technology changes since our last FISMA audit?	

Table A-2: Process walk-through requests

The OIG has identified the processes that we must understand according to FISMA domains under the assumption the processes listed under each domain are covered by the same agency personnel. If inaccurate, please let us know, and we can separate requests for coordination purposes.

Related FISMA domain and metric number	OIG request number	Request	Agency response
Risk Management ***Metrics 1–6, 10***	**7**	a. Information technology asset inventory process, including how to add, update, and remove items, as well as the information technology registry process. b. How risk-based resources are reviewed and allocated at the enterprise and system level. c. The control assessment process, including how the assessments are done, who has visibility over enterprise wide area network vulnerabilities, and what the timing of the review cycle is.	
Supply Chain Risk Management ***Metrics 14–15***	**8**	a. Processes or tools used to detect and prevent counterfeit components from entering the system. b. Procedures for maintaining configuration control over organizationally defined system components that are awaiting repair and service or repaired components awaiting return to service.	

Related FISMA domain and metric number	OIG request number	Request	Agency response
		c. Requirements and procedures for reporting counterfeit system components.	
Configuration Management ***Metrics 17, 18, 20, 21, 23***	**9**	a. Individual roles and responsibilities of configuration management stakeholders and what documentation is maintained. b. Process for creating, updating, and maintaining Agency configuration management plans. c. Process for managing software vulnerabilities, including the tracking, updating, and notification of parties. d. Process for developing, maintaining, and implementing configuration changed control activities.	
Identity and Access Management ***Metrics 28, 30, 31, 32***	**10**	a. Process for assigning risk designation roles and responsibilities, including personnel screening prior to Agency system access and the documentation that is created to support the delegation. b. Process for granting Agency system access for privileged and nonprivileged users, including the documentation that is created and maintained to support the access.	
Data Protection and Privacy ***Metrics 36-39***	**11**	a. Information technology processes used for encryption of data at rest, data in transit, and removable media for the enterprise wide area network. b. Data exfiltration and enhanced network defenses for the enterprise wide area network. c. Data breach response plan for the EPA, including how to deal with credit monitoring and repair services.	
Security Training ***Metrics 42, 44, 45***	**12**	a. Process for assessing the knowledge, skills, and abilities of the EPA's workforce to determine its awareness and specialized training needs. b. Security awareness training tracking and documentation. c. The process for developing, updating, and maintaining specialized security training documentation.	
Information Security Continuous Monitoring ***Metrics 47, 49, 50***	**13**	a. Vulnerability scanning tools and processes, including how vulnerabilities are tracked and remediated. b. Information Security Continuous Monitoring performance and reporting tools and processes, including what is reviewed, how often reviews are conducted, and to whom findings are sent for remediation.	
Incident Response ***Metrics 52–56***	**14**	a. Processes and tools use for incident response, including creating, updating, maintaining, disseminating, and documenting security incident reports.	

Related FISMA domain and metric number	OIG request number	Request	Agency response
Contingency Planning ***Metrics 61–64***	**15**	a. Process for drafting, updating, and maintaining a Business Impact Analysis, including what documentation is needed and maintained to support the decision. b. Process for drafting, updating, and maintaining information system contingency planning and testing exercises, including what documentation is need and maintained. c. Process for creating, disseminating, and maintaining backup and storage information, including the documentation that is maintained.	

APPENDIX B: FY 2024 IG FISMA Metrics

Note: These tables are copied from the Office of Management and Budget's *FY 2023–2024 Inspector General Federal Information Security Modernization Act (FISMA) Reporting Metrics.*

IDENTIFY FUNCTION AREA

Risk Management

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
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 800-37 (Rev. 2) • NIST SP 800-53 (Rev. 5): CA-3, PM-5, and CM-8 • NIST Cybersecurity Framework (CSF): ID.AM-1 – 4 • FY 2023 CIO FISMA Metrics: 1.1 and 1.5 • OMB A-130 • OMB M-23-03	Core Metric	The organization has not defined its policies, procedures, and processes for developing and maintaining a comprehensive and accurate inventory of its information systems and system interconnections.	The organization has defined its policies, procedures, and processes for developing and maintaining a comprehensive and accurate inventory of its information systems and system interconnections.	The organization consistently implements its policies, procedures, and processes to maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third-party systems), and system interconnections.	The organization ensures that the information systems included in its inventory are subject to the monitoring processes defined within the organization's ISCM strategy.	The organization uses automation to develop and maintain a centralized information system inventory that includes hardware and software components from all organizational information systems. The centralized inventory is updated in a near-real time basis.
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 800-37 (Rev. 2): Tasks P-10 and P-16 • NIST SP 800-53 (Rev. 5): CA-7 and CM-8 • NIST SP 800-137 • NIST SP 800-207 • NIST 1800-5 • NIST IR 8011 • NIST CSF: ID.AM-1 • Federal Enterprise Architecture (FEA) Framework • FY 2023 CIO FISMA Metrics: 1.2, 1.3, and 10.8 • CIS Top 18 Security Controls: Control 1 • OMB M-23-03 • DHS Binding Operational Directive (BOD) 23-01 • BOD 23-01 Implementation Guidance	Core Metric	The organization has not defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network (including through automated asset discovery) with the detailed information necessary for tracking and reporting.	The organization has defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network (including through automated asset discovery) with the detailed information necessary for tracking and reporting.	The organization consistently uses its standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network (including through automated asset discovery) and uses this taxonomy to inform which assets can/cannot be introduced into the network. The organization is making sufficient progress towards reporting at least 80% of its GFEs through DHS' CDM program.	The organization ensures that the hardware assets connected to the network are covered by an organization-wide hardware asset management capability and are subject to the monitoring processes defined within the organization's ISCM strategy. For mobile devices, the agency enforces the capability to deny access to agency enterprise services when security and operating system updates have not been applied within a given period based on agency policy or guidance.	The organization employs automation to track the life cycle of the organization's hardware assets with processes that limit the manual/procedural methods for asset management. Further, hardware inventories are regularly updated as part of the organization's enterprise architecture current and future states.
3. To what extent does the organization use standard data elements/taxonomy to develop and maintain	• NIST SP 800-37 (Rev. 2): Task P-10	Core Metric	The organization has not defined policies, procedures, and processes for using standard data	The organization has defined policies, procedures, and processes for using standard data elements/taxonomy to	The organization consistently uses its standard data elements/taxonomy to develop and maintain an up-	The organization ensures that the software assets, including EO-critical software and mobile applications as	The organization employs automation to track the life cycle of the organization's software assets (and their

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?	• NIST SP 800-53 (Rev. 5): CA-7, CM-8, CM-10, and CM-11 • NIST SP 800-137 • NIST SP 800-207: Section 7.3 • NIST 1800-5 • NIST IR 8011 • NIST Security Measures for EO-Critical Software Use • NIST CSF: ID.AM-2 • FEA Framework • FY 2023 CIO FISMA Metrics: 1.4 and 4.1 • OMB M-21-30 • OMB M-22-09 • OMB M-22-18 • OMB M-23-03 • CIS Top 18 Security Controls: Control 2 • CISA Cybersecurity Incident Response Playbooks		elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses, including for EO-critical software and mobile applications, used in the organization's environment with the detailed information necessary for tracking and reporting.	develop and maintain an up-to-date inventory of software assets and licenses, including for EO-critical software and mobile applications, used in the organization's environment with the detailed information necessary for tracking and reporting.	to-date inventory of software assets and licenses, including for EO-critical software and mobile applications, used in the organization's environment and uses this taxonomy to inform which assets can/cannot be introduced into the network. The organization establishes and maintains a software inventory for all platforms running EO-critical software and all software (both EO-critical and non-EO-critical) deployed to each platform.	appropriate, on the network (and their associated licenses), are covered by an organization-wide software asset management (or Mobile Device Management) capability and are subject to the monitoring processes defined within the organization's ISCM strategy. For mobile devices, the agency enforces the capability to prevent the execution of unauthorized software (e.g., blacklist, whitelist, or cryptographic containerization).	associated licenses), including for EO-critical software and mobile applications, with processes that limit the manual/procedural methods for asset management. Further, software inventories are regularly updated as part of the organization's enterprise architecture current and future states.
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 800-37 (Rev. 2): Tasks C-2, C-3, P-4, P-12, P-13, S-1 – S-3 • NIST SP 800-53 (Rev. 5): RA-2, PM-7, and PM-11 • NIST SP 800-60 • NIST IR 8170 • NIST CSF: ID.BE-3, ID.AM-5, and ID.SC-2 • FIPS 199 • FY 2023 CIO FISMA Metrics: 1.1 • OMB M-19-03	FY24	The organization has not defined policies, procedures, and processes for categorizing, reviewing, and communicating the importance/priority of information systems in enabling its missions and business functions, including for high value assets, as appropriate. In addition, the organization has not defined its policies, procedures, and processes for controls allocation, selection, and tailoring based on the importance/ priority of its information systems.	The organization has defined policies, procedures, and processes for categorizing, reviewing, and communicating the importance/priority of information systems in enabling its missions and business functions, including for high value assets, as appropriate. In addition, the organization has defined policies, procedures, and processes for controls allocation, selection and tailoring based on the importance/ priority of its information systems.	The organization consistently implements its policies, procedures, and processes for system categorization, review, and communication, including for high value assets, as appropriate. Security categorizations consider potential adverse impacts to organization operations, organizational assets, individuals, other organizations, and the Nation. System categorization levels are used to guide risk management decisions, such as the allocation, selection, and implementation of appropriate control baselines.	The organization ensures the risk-based allocation of resources based on system categorization, including for the protection of high value assets, as appropriate, through collaboration and data-driven prioritization.	The organization uses impact-level prioritization for additional granularity, and cybersecurity framework profiles, as appropriate, to support risk-based decision-making.

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
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 800-37 (Rev. 2): Tasks P-2, P-3, P-14, R-2, and R-3 • NIST SP 800-39 • NIST SP 800-53 (Rev. 5): RA-3 and PM-9 • NIST IR 8286 • NIST IR 8286A • NIST IR 8286B • NIST IR 8286C • NIST IR 8286D • NIST CSF: ID RM-1 – ID.RM-3 • OMB A-123 • OMB M-16-17 • OMB M-23-03	Core Metric	The organization has not defined and communicated the policies, procedures and processes it uses to manage the cybersecurity risks associated with operating and maintaining its information systems. At a minimum, the policies, procedures, and processes do not cover the following areas from a cybersecurity perspective: • Risk framing • Risk assessment • Risk response • Risk monitoring	The organization has defined and communicated the policies, procedures and processes it uses to manage the cybersecurity risks associated with operating and maintaining its information systems. The policies, procedures, and processes cover cybersecurity risk management at the organizational, mission/business process, and information system levels and address the following components • Risk framing • Risk assessment • Risk response • Risk monitoring	The organization consistently implements its policies, procedures, and processes to manage the cybersecurity risks associated with operating and maintaining its information systems. The organization ensures that decisions to manage cybersecurity risk at the information system level are informed and guided by risk decisions made at the organizational and mission/business levels. System risk assessments are performed [according to organizational defined time frames] and appropriate security controls to mitigate risks identified are implemented on a consistent basis. The organization uses the common vulnerability scoring system, or similar approach, to communicate the characteristics and severity of software vulnerabilities. Further, the organization uses a cybersecurity risk register to manage risks, as appropriate, and is consistently capturing and sharing lessons learned on the effectiveness of cybersecurity risk management processes and updating the program accordingly.	The organization uses the results of its system level risk assessments, along with other inputs, to perform and maintain an organization-wide cybersecurity and privacy risk assessment. The result of this assessment is documented in a cybersecurity risk register and serve as an input into the organization's enterprise risk management program. The organization consistently monitors the effectiveness of risk responses to ensure that risk tolerances are maintained at an appropriate level. The organization ensures that information in cybersecurity risk registers is obtained accurately, consistently, and in a reproducible format and is used to (i) quantify and aggregate security risks, (ii) normalize cybersecurity risk information across organizational units, and (iii) prioritize operational risk response.	The cybersecurity risk management program is fully integrated at the organizational, mission/business process, and information system levels, as well as with the entity's enterprise risk management program. Further, the organization's cybersecurity risk management program is embedded into daily decision making across the organization and provides for continuous identification and monitoring to ensure that risk remains within organizationally-defined acceptable levels. The organization uses Cybersecurity Framework profiles and enterprise risk profiles to align cybersecurity outcomes with mission or business requirements, risk tolerance, and resources of the organization.
6. To what extent does the organization use an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the	• NIST SP 800-37 (Rev. 2): Task P-16 • NIST SP 800-39 • NIST SP 800-53 (Rev. 5): PL-8, SA-3, SA-8. SA-9, SA-12, and PM-9 • NIST SP 800-160 • NIST SP 800-163, (Rev. 1) • NIST SP 800-218	FY24	The organization has not defined an information security architecture and its processes for ensuring that new/acquired hardware/software, including mobile apps, are consistent with its security architecture prior	The organization has defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture.	The organization has consistently implemented its security architecture across the enterprise, business process, and system levels. System security engineering principles are followed and include assessing the impacts to the organizations	The organization's information security architecture is integrated with its systems development lifecycle and defines and directs implementation of security methods, mechanisms, and capabilities to both the Information and	The organization uses advanced technologies and techniques for managing supply chain risks. To the extent practicable, the organization can quickly adapt its information security and enterprise

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
organization's supply chain?	• NIST CSF: ID.SC-1 and PR.IP-2 • FEA Framework • OMB M-15-14 • OMB M-19-03 • OMB M-22-18 • SECURE Technology Act: s. 1326 • Federal Information Technology Acquisition Reform Act (FITARA)		to introducing systems into its development environment.	In addition, the organization has defined how it implements system security engineering principles and software assurance processes for mobile applications, within its system development life cycle (SDLC).	information security architecture prior to introducing information system changes into the organization's environment. In addition, the organization employs a software assurance process for mobile applications.	Communications Technology (ICT) supply chain and the organization's information systems.	architectures to mitigate supply chain risks.
10. To what extent does the organization use 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 • NIST SP 800-207: Tenets 5 and 7 • NIST IR 8286 • OMB A-123 • OMB M-22-09 • CISA Zero Trust Maturity Model: Pillars 2-4 • FY 2023 CIO FISMA Metrics: 7.4.2	Core Metric	The organization has not identified and defined its requirements for an automated solution to provide a centralized, enterprise wide (portfolio) view of cybersecurity risks across the organization, including risk control and remediation activities, dependences, risk scores/levels, and management dashboards.	The organization has identified and defined its requirements for an automated solution that provides a centralized, enterprise-wide view of cybersecurity risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards.	The organization consistently implements an automated solution across the enterprise that provides a centralized, enterprise-wide view of cybersecurity risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. All necessary sources of cybersecurity risk information are integrated into the solution.	In addition, the organization ensures that cybersecurity risk management information is integrated into ERM reporting tools (such as a governance, risk management, and compliance tool), as appropriate.	The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its cybersecurity risk management program. Examples include scenario analysis and modeling, the incorporation of technical indicators from threat intelligence, and the ability to consume open security control assessments language (OSCAL) into its GRC processes.

Supply Chain Risk Management (SCRM)

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
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?	• NIST SP 800-53 (Rev. 5): SA-4, SR-3, SR-5, and SR-6 • NIST SP 800-152 • NIST SP 800-161 (Rev. 1) • NIST SP 800-218: Task PO.1.3 • NIST IR 8276 • NIST CSF: ID.SC-2 through ID.SC-4 • OMB A-130 • OMB M-19-03 • OMB M-22-18 • CIS Top 18 Security Controls: Control 15 • The Federal Acquisition Supply Chain Security Act of 2018	Core Metric	The organization has not defined and communicated policies, procedures, and processes to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements.	The organization has defined and communicated policies and procedures to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements. The following components, at a minimum, are defined • The identification and prioritization of externally provided systems, system components, and services as well how the organization	The organization ensures that its policies, procedures, and processes are consistently implemented for assessing and reviewing the supply chain-related risks associated with suppliers or contractors and the system, system component. In addition, the organization obtains sufficient assurance, through audits, test results, software producer self-attestation (in accordance with M-22-18), or other forms of evaluation, that the security and supply chain	The organization uses qualitative and quantitative performance metrics (e.g., those defined within SLAs) to measure, report on, and monitor the information security and SCRM performance of organizationally defined products, systems, and services provided by external providers. In addition, the organization has incorporated supplier risk evaluations, based on criticality, into its continuous monitoring practices to	The organization analyzes, in a near-real time basis, the impact of material changes to security and SCRM assurance requirements on its relationships with external providers and ensures that acquisition tools, methods, and processes are updated as soon as possible.

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
	• FedRAMP standard contract clauses • Cloud computing contract best practices • DHS's ICT Supply Chain Library			maintains awareness of its upstream suppliers. • Integration of acquisition processes, including the use of contractual agreements that stipulate appropriate cyber and SCRM measures for external providers. • Tools and techniques to use the acquisition process to protect the supply chain, including, risk-based processes for evaluating cyber supply chain risks associated with third party providers, as appropriate. • Contract tools or procurement methods to confirm contractors are meeting their contractual SCRM obligations.	controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and applicable NIST guidance. Furthermore, the organization maintains visibility into its upstream suppliers and can consistently track changes in suppliers.	maintain situational awareness into the supply chain risks.	
15. To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems?	• NIST SP 800-53 (Rev. 5): SR-11 (1)(2) • NIST SP 800-161 (Rev. 1) • OMB M-22-18 • NIST SP 800-218	FY24	The organization has not defined and communicated its component authenticity policies and procedures.	The organization has defined and communicated its component authenticity policies and procedures. At a minimum the following areas are addressed: • Procedures to detect and prevent counterfeit components from entering the system. • Procedures to maintain configuration control over organizationally defined system components that are awaiting repair and service or repaired components awaiting return to service. • Requirements and procedures for reporting counterfeit system components.	The organization consistently implements its component authenticity policies and procedures. Further, the organization: • Provides component authenticity/anti-counterfeit training for designated personnel. • Maintains configuration control over organizationally defined system components that are awaiting repair and service or repaired components awaiting return to service.	The organization monitors, analyzes, and reports on the qualitative and quantitative performance measures used to gauge the effectiveness of its component authenticity policies and procedures and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format. In addition, the organization has incorporated component authenticity controls into its continuous monitoring practices.	In a near real-time basis, the organization can update its supply chain risk management policies and procedures, as appropriate, to respond to evolving and sophisticated threats.

PROTECT FUNCTION AREA

Configuration Management

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
17. To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?	• NIST SP 800-53 (Rev. 5): CM-1 • NIST SP 800-128: Section 2.4 • Green Book: Principles 3, 4, and 5	FY24	Roles and responsibilities at the organizational and information system levels for stakeholders involved in information system configuration management have not been fully defined and communicated across the organization.	Roles and responsibilities at the organizational and information system levels for stakeholders involved in information system configuration management have been fully defined and communicated across the organization.	Individuals are performing the roles and responsibilities that have been defined across the organization.	Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively perform information system configuration management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	The organization continuously evaluates and adapts its configuration management-based roles and responsibilities to account for a changing cybersecurity landscape.
18. To what extent does the organization use 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 800-53 (Rev. 5): CM-9 • NIST SP 800-128: Section 2.3.2	FY24	The organization has not developed an organization wide configuration management plan with the necessary components.	The organization has developed an organization wide configuration management plan that includes the necessary components.	The organization has consistently implemented an organization wide configuration management plan and has integrated its plan with its risk management and continuous monitoring programs. Further, the organization uses lessons learned in implementation to make improvements to its plan.	The organization monitors, analyzes, and reports to stakeholders qualitative and quantitative performance measures on the effectiveness of its configuration management plan, uses this information to take corrective actions when necessary, and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.	The organization uses automation to adapt its configuration management plan and related processes and activities to a changing cybersecurity landscape on a near real-time basis (as defined by the organization).
20. To what extent does the organization use configuration settings/common secure configurations for its information systems?	• NIST SP 800-53 (Rev. 5): CM-6, CM-7, RA-5, and SI-2 • NIST SP 800-70 (Rev. 4) • NIST CSF: ID.RA-1 and DE.CM-8 • NIST Security Measures for EO-Critical Software Use: SM 3.3 • OMB M-22-09	Core Metric	The organization has not established policies and procedures for ensuring that configuration settings/common secure configurations are defined, implemented, and monitored.	The organization has developed, documented, and disseminated its policies and procedures for configuration settings/common secure configurations. In addition, the organization has developed, documented, and disseminated common	The organization consistently implements, assesses, and maintains secure configuration settings for its information systems based on the principle of least functionality.	The organization employs automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to the organization's network and	The organization deploys system configuration management tools that automatically enforce and redeploy configuration settings to systems at frequent intervals as defined by the

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
	• OMB M-23-03 • BOD 23-01 • CIS Top 18 Security Controls: Controls 4 and 7 • CISA Cybersecurity Incident Response Playbooks			secure configurations (hardening guides) that are tailored to its environment. Further, the organization has established a deviation process.	Further, the organization consistently uses SCAP-validated software assessing (scanning) capabilities against all systems on the network (in accordance with BOD 23-01) to assess and manage both code-based and configuration-based vulnerabilities. The organization uses lessons learned in implementation to make improvements to its secure configuration policies and procedures.	makes appropriate modifications in accordance with organization-defined timelines.	organization, or on an event driven basis.
21. To what extent does the organization use flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities on all network addressable IP-assets?	• NIST SP 800-40 (Rev. 4) • NIST SP 800-53 (Rev. 5): CM-3, RA-5, SI-2, and SI-3 • NIST SP 800-207: Section 2.1 • NIST CSF: ID.RA-1 • NIST Security Measures for EO-Critical Software Use: SM 3.2 • OMB M-22-09 • FY 2023 CIO FISMA Metrics: 1.4, 8.1 and 8.2 • CIS Top 18 Security Controls: Controls 4 and 7 • BOD 18-02 • BOD 19-02 • BOD 22-01 • BOD 23-01 • BOD 23-01 Implementation Guidance • CISA Cybersecurity Incident Response Playbooks	Core Metric	The organization has not developed, documented, and disseminated its policies and procedures for flaw remediation, including for mobile devices (GFE and non-GFE).	The organization has developed, documented, and disseminated its policies and procedures for flaw remediation, including for mobile devices. Policies and procedures include processes for: identifying, reporting, and correcting information system flaws, testing software and firmware updates prior to implementation, installing security relevant updates and patches within organizational-defined timeframes, and incorporating flaw remediation into the organization's configuration management processes.	The organization consistently implements its flaw remediation policies, procedures, and processes and ensures that patches, hotfixes, service packs, and anti-virus/malware software updates are identified, prioritized, tested, and installed in a timely manner. In addition, the organization patches critical vulnerabilities within 30 days and uses lessons learned in implementation to make improvements to its flaw remediation policies and procedures. Further, for EO-critical software platforms and all software deployed to those platforms, the organization uses supported software versions.	The organization centrally manages its flaw remediation process and uses automated patch management and software update tools for operating systems, where such tools are available and safe. The organization monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of flaw remediation processes and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.	The organization uses automated patch management and software update tools for all applications and network devices (including mobile devices), as appropriate, where such tools are available and safe. As part its flaw remediation processes, the organization performs deeper analysis of software code, such as through patch sourcing and testing.
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	• NIST SP 800-53 (Rev. 5): CM-2, CM-3, and CM-4 • NIST CSF: PR.IP-3	FY24	The organization has not developed, documented, and disseminated its policies and procedures for managing configuration change control. Policies and procedures do not address, at a minimum, the necessary configuration change control related activities.	The organization has developed, documented, and disseminated its policies and procedures for managing configuration change control. The policies and procedures address, at a minimum, the necessary configuration change control related activities.	The organization consistently implements its change control policies, procedures, and processes, including explicit consideration of security impacts prior to change implementation. The organization uses lessons learned in implementation to make	The organization monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its change control activities and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.	The organization uses automation to improve the accuracy, consistency, and availability of configuration change control and configuration baseline information. Automation is also used to provide data aggregation and correlation capabilities, alerting mechanisms, and dashboards on change

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
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?					improvements to its change control policies and procedures.	In addition, the organization implements [organizationally defined security responses] if baseline configurations are changed in an unauthorized manner.	control activities to support risk-based decision making across the organization.

Identity and Access Management

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
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. 5): PS-2 and PS-3 • NIST CSF: PR.IP-11 • OMB M-19-17 • National Insider Threat Policy • FY 2023 CIO FISMA Metrics: 7.4.3	FY24	The organization has not defined its processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems.	The organization has defined its processes for ensuring that all personnel are assigned risk designations and appropriately screened prior to being granted access to its systems. Processes have been defined for assigning risk designations for all positions, establishing screening criteria for individuals filling those positions, authorizing access following screening completion, and rescreening individuals on a periodic basis.	The organization ensures that all personnel are assigned risk designations, appropriately screened prior to being granted system access, and rescreened periodically.	The organization employs automation to centrally document, track, and share risk designations and screening information with necessary parties.	On a near-real time basis, the organization evaluates personnel security information from various sources, integrates this information with anomalous user behavior data (audit logging) and/or its insider threat activities, and adjusts permissions accordingly.
30. To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for non-privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?	• NIST SP 800-53 (Rev. 5): AC-17, IA-2, IA-5, IA-8, and PE-3 • NIST SP 800-63 • NIST SP 800-128 • NIST SP 800-157 • NIST SP 800-207: Tenet 6 • NIST CSF: PR.AC-1 and PR.AC-6 • NIST Security Measures for EO-Critical Software Use: SM 1.1 • FIPS 201-2 • HSPD-12	Core Metric	The organization has not planned for the use of strong authentication mechanisms for non-privileged users of the organization's facilities [organization-defined entry/exit points], systems, and networks, including for remote access. In addition, the organization has not performed digital identity risk assessments to determine which systems	The organization has planned for the use of strong authentication mechanisms for non-privileged users of the organization's facilities [organization-defined entry/exit points], systems, and networks, including the completion of digital identity risk assessments.	The organization has consistently implemented strong authentication mechanisms for non-privileged users of the organization's facilities [organization-defined entry/exit points] and networks, including for remote access, in accordance with Federal targets. For instances where it would be impracticable to use the PIV card, the organization	All non-privileged users use strong authentication mechanisms to authenticate to applicable organizational systems and facilities [organization-defined entry/exit points]. To the extent possible, the organization centrally implements support for non-PIV authentication mechanisms in their enterprise identity management system.	The organization has implemented an enterprise-wide single sign on solution and all the organization's systems interface with the solution, resulting in an ability to manage user (non-privileged) accounts and privileges centrally and report on effectiveness on a near real-time basis.

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
	• OMB M-19-17 • OMB M-22-09 • OMB M-23-03 • CIS Top 18 Security Controls: Control 6 • CISA Capacity Enhancement Guide • FY 2023 CIO FISMA Metrics: 2.3, 2.3.1, 2.3.2, 2.4, 2.9, 2.10, and 2.10.2		require strong authentication.		uses an alternative token (derived PIV credential) which can be implemented and deployed with mobile devices. Further, for public-facing systems that support multifactor authentication, users are provided the option of using phishing-resistant multifactor authentication.		
31. To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?	• NIST SP 800-53 (Rev. 5): AC-17 and PE-3 • NIST SP 800-63 • NIST SP 800-128 • NIST SP 800-157 • NIST SP 800-207: Tenet 6 • NIST CSF: PR.AC-1 and PR.AC-6 • NIST Security Measures for EO-Critical Software Use: SM 1.1 • FIPS 201-2 • HSPD-12 • OMB M-19-17 • OMB M-22-09 • OMB M-23-03 • DHS ED 19-01 • CIS Top 18 Security Controls: Control 6 • FY 2023 CIO FISMA Metrics: 2.3, 2.4, 2.9, and 2.10	Core Metric	The organization has not planned for the use of strong authentication mechanisms for privileged users of the organization's facilities [organization-defined entry/exit points], systems, and networks, including for remote access. In addition, the organization has not performed digital identity risk assessments to determine which systems require strong authentication.	The organization has planned for the use of strong authentication mechanisms for privileged users of the organization's facilities [organization-defined entry/exit points], systems, and networks, including the completion of digital identity risk assessments.	The organization has consistently implemented strong authentication mechanisms for privileged users of the organization's facilities [organization-defined entry/exit points], and networks, including for remote access, in accordance with Federal targets. For instances where it would be impracticable to use the PIV card, the organization uses an alternative token (derived PIV credential) which can be implemented and deployed with mobile devices.	All privileged users, including those who can make changes to DNS records, use strong authentication mechanisms to authenticate to applicable organizational systems.	The organization has implemented an enterprise-wide single sign on solution and all the organization's systems interface with the solution, resulting in an ability to manage user (privileged) accounts and privileges centrally and report on effectiveness on a near real-time basis.
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	• NIST SP 800-53 (Rev. 5): AC-1, AC-2, AC-5, AC-6, AC-17, AU-2, AU-3, AU-6, and IA-4 • NIST CSF PR.AC-4 • NIST Security Measures for EO-Critical Software Use: SM 2.2 • FY 2023 CIO FISMA Metrics: 3.1 • OMB M-19-17 • OMB M-21-31 • DHS ED 19-01 • CIS Top 18 Security Controls: Controls 5, 6, and 8	Core Metric	The organization has not defined its processes for provisioning, managing, and reviewing privileged accounts.	The organization has defined its processes for provisioning, managing, and reviewing privileged accounts. Defined processes cover approval and tracking; inventorying and validating; and logging and reviewing privileged users' accounts.	The organization ensures that its processes for provisioning, managing, and reviewing privileged accounts are consistently implemented across the organization. The organization limits the functions that can be performed when using privileged accounts; limits the duration that privileged accounts can be logged in; and ensures that privileged user activities are logged and periodically reviewed.	The organization employs automated mechanisms (e.g., machine-based, or user-based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate. Further, the organization is meeting privileged identity and credential management logging requirements at maturity EL2, in accordance with M-21-31.	The organization is making demonstrated progress towards implementing EL3's advanced requirements for user behavior monitoring to detect and alert on privileged user compromise.

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
account activities are logged and periodically reviewed?							

Data Protection and Privacy

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
36. To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? • Encryption of data at rest • Encryption of data in transit • Limitation of transfer to removable media • Sanitization of digital media prior to disposal or reuse	• NIST SP 800-37 (Rev. 2) • NIST SP 800-53 (Rev. 5): SC-8, SC-28, MP-3, MP-6, and SI-12(3) • NIST SP 800-207 • NIST CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6 • NIST Security Measures for EO-Critical Software Use: SM 2.3 and SM 2.4 • OMB M-22-09 • DHS BOD 18-02 • FY 2023 CIO FISMA Metrics: 2.1, 2.1.1 and 2.2 • CIS Top 18 Security Controls: Control 3	Core Metric	The organization has not defined its policies and procedures in one or more of the specified areas.	The organization's policies and procedures have been defined and communicated for the specified areas. Further, the policies and procedures have been tailored to the organization's environment and include specific considerations based on data classification and sensitivity.	The organization's policies and procedures have been consistently implemented for the specified areas, including (i) use of FIPS-validated encryption of PII and other agency sensitive data, as appropriate, both at rest and in transit, (ii) prevention and detection of untrusted removable media, and (iii) destruction or reuse of media containing PII or other sensitive agency data.	The organization ensures that the security controls for protecting PII and other agency sensitive data, as appropriate, throughout the data lifecycle are subject to the monitoring processes defined within the organization's ISCM strategy.	The organization employs advanced capabilities to enhance protective controls, including: • Remote wiping • Dual authorization for sanitization of media devices • Exemption of media marking as long as the media remains within organizationally-defined control areas • Configuring systems to record the date the PII was collected, created, or updated and when the data is to be deleted or destroyed according to an approved data retention schedule.
37. To what extent has the organization implemented security controls (e.g., EDR) to prevent data exfiltration and enhance network defenses?	• NIST SP 800-53 (Rev. 5): SI-3, SI-7(8), SI-4(4)(18), SC-7(10), and SC-18 • NIST CSF: PR.DS-5 • NIST Security Measures for EO-Critical Software Use: SM 4.3 • OMB M-21-07 • OMB M-22-01 • CIS Top 18 Security Controls: Controls 9 and 10 • DHS BOD 18-01 • DHS ED 19-01	Core Metric	The organization has not defined its policies and procedures related to data exfiltration, endpoint detection and response, enhanced network defenses, email authentication processes, and mitigation against DNS infrastructure tampering.	The organization has defined and communicated it policies and procedures for data exfiltration, endpoint detection and response, enhanced network defenses, email authentication processes, and mitigation against DNS infrastructure tampering.	The organization consistently monitors inbound and outbound network traffic, ensuring that all traffic passes through a web content filter that protects against phishing, malware, and blocks against known malicious sites. Additionally, the organization checks outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII. Also, suspected malicious traffic is quarantined or blocked. In addition, the organization uses email authentication technology and ensures the	The organization analyzes qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses. The organization also conducts exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses. Further, the organization monitors its DNS infrastructure for potential tampering, in accordance with its ISCM strategy. In addition, the organization audits its DNS records. Further, the organization has assessed its current EDR capabilities, identified any	The organization's data exfiltration and enhanced network defenses are fully integrated into the ISCM and incident response programs to provide near real-time monitoring of the data that is entering and exiting the network, and other suspicious inbound and outbound communications. The organization continuously runs device posture assessments (e.g., using EDR tools) to maintain visibility and analytics capabilities related to data exfiltration.

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
					use of valid encryption certificates for its domains. The organization consistently implements EDR capabilities to support host-level visibility, attribution, and response for its information systems.	gaps, and is coordinating with CISA for future EDR solution deployments.	
38. To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events?	• NIST SP 800-53 (Rev. 5): IR-8 and IR-8(1) • NIST SP 800-122 • OMB M-17-12 • OMB M-23-03 • FY 2022 SAOP FISMA Metrics: Section 12	FY24	The organization has not developed a Data Breach Response Plan that includes the agency's policies and procedures for reporting, investigating, and managing a privacy-related breach. Further, the organization has not established a breach response team that includes the appropriate agency officials.	The organization has defined and communicated its Data Breach Response Plan, including its processes and procedures for data breach notification. Further, a breach response team has been established that includes the appropriate agency officials.	The organization consistently implements its Data Breach Response plan. Additionally, the breach response team participates in table-top exercises and uses lessons learned to make improvements to the plan as appropriate. Further, the organization can identify the specific individuals affected by a breach, send notice to the affected individuals, and provide those individuals with credit monitoring and repair services, as necessary.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization's Data Breach Response plan is fully integrated with incident response, risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. Further the organization employs automation to monitor for potential privacy incidents and takes immediate action to mitigate the incident and provide protection to the affected individuals.
39. To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)	• NIST SP 800-53 (Rev. 5): AT-1, AT-2, AT-3, and PL-4 • FY 2022 SAOP FISMA Metrics: Section 9, 10, and 11	FY24	The organization has not defined its privacy awareness training program based on organizational requirements, its mission, and the types of PII that its users have access to. In addition, the organization has not developed role-based privacy training for individuals having responsibility for PII or activities involving PII.	The organization has defined and communicated its privacy awareness training program, including requirements for role-based privacy awareness training. Further, training has been tailored to the organization's mission and risk environment.	The organization ensures that all individuals receive basic privacy awareness training and individuals having responsibilities for PII or activities involving PII receive role-based privacy training at least annually. Additionally, the organization ensures that individuals certify acceptance of responsibilities for privacy requirements at least annually.	The organization measures the effectiveness of its privacy awareness training program by obtaining feedback on the content of the training and conducting targeted phishing exercises for those with responsibility for PII. Additionally, the organization make updates to its program based on statutory, regulatory, mission, program, business process, information system requirements, and/or results from monitoring and auditing.	The organization has institutionalized a process of continuous improvement incorporating advanced privacy training practices and technologies.

Security Training

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
42. To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover?	• NIST SP 800-50: Section 3.2 • NIST SP 800-53 (Rev. 5): AT-2, AT-3, and PM-13 • NIST SP 800-181 • Federal Cybersecurity Workforce Assessment Act of 2015 • National Cybersecurity Workforce Framework • CIS Top 18 Security Controls: Control 14 • FY 2023 CIO FISMA Metrics: 6.1 • EO 13870	Core Metric	The organization has not defined its processes for assessing the knowledge, skills, and abilities of its workforce.	The organization has defined its processes for assessing the knowledge, skills, and abilities of its workforce to determine its awareness and specialized training needs and periodically updating its assessment to account for a changing risk environment.	The organization has assessed the knowledge, skills, and abilities of its workforce; tailored its awareness and specialized training; and has identified its skill gaps. Further, the organization periodically updates its assessment to account for a changing risk environment. In addition, the assessment serves as a key input to updating the organization's awareness and training strategy/plans.	The organization has addressed its identified knowledge, skills, and abilities gaps through training or talent acquisition.	The organization's personnel collectively possess a training level such that the organization can demonstrate that security incidents resulting from personnel actions or inactions are being reduced over time.
44. To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting?	• NIST SP 800-50: 6.2 • NIST SP 800-53 (Rev. 5): AT-1 and AT-2 • NIST CSF: PR.AT-2 • CIS Top 18 Security Controls: Control 14	FY24	The organization has not defined its security awareness policies, procedures, and related material based on its mission, risk environment, and the types of information systems that its users have access to. In addition, the organization has not defined its processes for ensuring that all information system users are provided security awareness training [within organizationally defined timeframes] and periodically thereafter. Furthermore, the organization has not defined its processes for evaluating and obtaining feedback on its security awareness and training program and using that information to make continuous improvements.	The organization has defined and tailored its security awareness policies, procedures, and related material and delivery methods based on FISMA requirements, its, and the types of information systems that its users have access to. In addition, the organization has defined its processes for ensuring that all information system users including contractors are provided security awareness training [within organizationally defined timeframes] and periodically thereafter. Furthermore, the organization has defined its processes for evaluating and obtaining feedback on its security awareness and training program and using that information to make continuous improvements.	The organization ensures that its security awareness policies and procedures are consistently implemented. The organization ensures that all appropriate users complete the organization's security awareness training (or a comparable awareness training for contractors) [within organizationally defined timeframes] and periodically thereafter and maintains completion records. The organization obtains feedback on its security awareness and training program and uses that information to make improvements.	The organization measures the effectiveness of its awareness program by, for example, conducting phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate. The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness policies, procedures, and practices. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization has institutionalized a process of continuous improvement incorporating advanced security awareness practices and technologies. On a near real-time basis (as determined by the agency given its threat environment), the organization actively adapts its security awareness policies, procedures, processes to a changing cybersecurity landscape and provides awareness and training, as appropriate, on evolving and sophisticated threats.
45. To what extent does the organization ensure that specialized security training is provided to	• NIST SP 800-53 (Rev. 5): AT-3 and AT-4 • EO 13870	FY24	The organization has not defined its security training policies, procedures, and related	The organization has defined its security training policies, procedures, and related material based on FISMA	The organization ensures that its security training policies and procedures are consistently implemented.	The organization obtains feedback on its specialized security training content and processes and makes updates	The organization has institutionalized a process of continuous improvement incorporating advanced

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
individuals with significant security responsibilities (as defined in the organization's security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301)?	• 5 Code of Federal Regulation 930.301		materials based on its mission, risk environment, and the types of roles with significant security responsibilities. In addition, the organization has not defined its processes for ensuring that personnel with significant security roles and responsibilities are provided specialized security training [within organizationally defined timeframes] and periodically thereafter.	requirements, its mission and risk environment, and the types of roles with significant security responsibilities. In addition, the organization has defined its processes for ensuring that personnel with assigned security roles and responsibilities are provided specialized security training [within organizationally defined time frames] and periodically thereafter.	The organization ensures that individuals with significant security responsibilities complete the organization's defined specialized security training (or comparable training for contractors) [within organizationally defined timeframes] and periodically thereafter. The organization also maintains completion records for specialized training taken by individuals with significant security responsibilities. The organization obtains feedback on its security training program and uses that information to make improvements.	to its program, as appropriate. In addition, the organization measures the effectiveness of its specialized security training program by, for example, conducting targeted phishing exercises and following up with additional training, and/or disciplinary action, as appropriate. The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security training policies, procedures, and practices. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	security training practices and technologies. On a near real-time basis, the organization actively adapts its security training policies, procedures, processes to a changing cybersecurity landscape and provides awareness and training, as appropriate, on evolving and sophisticated threats.

DETECT FUNCTION AREA

Information Security Continuous Monitoring (ISCM)

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
47. To what extent does the organization use information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?	• NIST SP 800-37 (Rev. 2): Task P-7 • NIST SP 800-53 (Rev. 5): CA-7, PM-6, PM-14, and PM-31 • NIST SP 800-137: Sections 3.1 and 3.6 • NIST Security Measures for EO-Critical Software Use: SM 4.2 • CIS Top 18 Security Controls: Control 13	Core Metric	The organization has not developed, tailored, and communicated its ISCM policies and an organization wide ISCM strategy.	The organization has developed, tailored, and communicated its ISCM policies and strategy. The following areas are included: • Monitoring requirements at each organizational tier • The minimum monitoring frequencies for implemented controls across the organization (The criteria for determining minimum frequencies is established in coordination with organizational officials [e.g., senior accountable official for risk management, system owners, and common control	The organization's ISCM policies and strategy are consistently implemented at the organization, business process, and information system levels. In addition, the strategy supports clear visibility into assets, awareness into vulnerabilities, up-to-date threat information, and mission/business impacts. The organization also consistently captures lessons learned to make	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM policies and strategy and makes updates, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. The organization has transitioned to ongoing control and system authorization through the implementation of its	The organization's ISCM policies and strategy are fully integrated with its enterprise and supply chain risk management, configuration management, incident response, and business continuity programs. The organization can demonstrate that it is using its ISCM policies and strategy to reduce the cost and increase the efficiency of security and privacy programs.

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
				providers] and in accordance with organizational risk tolerance). • The organization's ongoing control assessment approach • How ongoing assessments are to be conducted • Analyzing ISCM data, reporting findings, and reviewing and updating the ISCM policies, procedures, and strategy	improvements to the ISCM policies and strategy.	continuous monitoring policies and strategy.	
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?	• NIST SP 800-18 (Rev. 1) • NIST SP 800-37 (Rev. 2): Task S-5 • NIST SP 800-53 (Rev. 5): CA-2, CA-5, CA-6, CA-7, PL-2, and PM-10 • NIST SP 800-137: Section 2.2 • NIST IR 8011 • NIST IR 8397 • OMB A-130 • OMB M-14-03 • OMB M-19-03 • OMB M-22-09 • FY 2023 CIO FISMA Metrics: 7.1	Core Metric	The organization has not developed system level continuous monitoring strategies/policies that define its processes for performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans, monitoring security controls for individual systems; and time-based triggers for ongoing authorization.	The organization has developed system level continuous monitoring strategies/policies that define its processes for performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans; monitoring security controls for individual systems; and time-based triggers for ongoing authorization. The system level strategy/policies address the monitoring of those controls that are not addressed by the organizational level strategy, as well as how changes to the system are monitored and reported.	The organization consistently implements its system level continuous monitoring strategies and related processes, including performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring security controls to provide a view of the organizational security posture, as well as each system's contribution to said security posture. In conjunction with the overall ISCM strategy, all security control classes (management, operational, and technical) and types (common, hybrid, and system-specific) are assessed and monitored, and their status updated regularly (as defined in the agency's information security policy) in security plans.	The organization uses the results of security control assessments and monitoring to maintain ongoing authorizations of information systems, including the maintenance of system security plans. Organization authorization processes include automated analysis tools and manual expert analysis, as appropriate.	The organization's system level ISCM policies and strategies are fully integrated with its enterprise and supply chain risk management, configuration management, incident response, and business continuity programs. The organization can demonstrate that it is using its system level ISCM policies and strategy to reduce the cost and increase the efficiency of security and privacy programs.
50. How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings?	• NIST SP 800-137	FY24	The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. Further, the	The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. In addition, the organization has defined the	The organization is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting.	The organization can integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of	On a near real-time basis, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
			organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions.	format of reports, frequency of reports, and the tools used to provide information to individuals with significant security responsibilities.		operations and security domains.	

RESPOND FUNCTION AREA

Incident Response

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
52. To what extent does the organization use an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents?	• NIST SP 800-53 (Rev. 5): IR-8 • NIST SP 800-61 (Rev. 2): Section 2.3.2 • NIST CSF: RS.RP-1 • Presidential Policy Directive (PPD) 8 – National Preparedness • FY 2023 CIO FISMA Metrics: 10.1.1 • FY 2022 CIO FISMA Metrics: 10.6	FY24	The organization has not developed an incident response plan to provide a roadmap for implementing its incident response capability.	The organization has developed a tailored incident response plan that addresses: • Structure and organization of the incident response capability • High-level approach for how the incident response capability fits into the overall organization • Defines reportable incidents, including major incidents • Metrics for measuring the incident response capability • Resources and management support	The organization consistently implements its incident response plan. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident response plan and making updates as necessary.	The organization monitors and analyzes the qualitative and quantitative performance measures that have been defined in its incident response plan to monitor and maintain the effectiveness of its overall incident response capability. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization's incident response plan is fully integrated with risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. In addition, the organization make near real-time updates to its incident response plan based on changing risk environments and threat information. The organization participates in DHS's Cyber Storm national level exercise, as appropriate, or other exercises, to assess, cybersecurity preparedness, and examine incident response processes.
53. To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been	• NIST SP 800-53 (Rev. 5) IR-7 • NIST SP 800-61 (Rev. 2) • NIST SP 800-83 • NIST CSF: RS.CO-1 • OMB M-20-04	FY24	Roles and responsibilities have not been fully defined and communicated across the organization, including appropriate levels of	The organization has defined and communicated the structures of its incident response teams, roles and responsibilities of incident response stakeholders, and associated levels of authority	Individuals are performing the roles and responsibilities that have been defined across the organization.	Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement incident response activities. Further, stakeholders are	The organization continuously evaluates and adapts its incident response-based roles and responsibilities to account for a changing cybersecurity landscape.

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
defined, communicated, and implemented across the organization?	• US-CERT Federal Incident Notification Guidelines • Green Book: Principles 3, 4, and 5		authority and dependencies.	and dependencies. In addition, the organization has designated a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities.		held accountable for carrying out their roles and responsibilities effectively.	
54. How mature are the organization's processes for incident detection and analysis?	• NIST SP 800-53 (Rev. 5): IR-4, IR-5, and IR-6 • NIST SP 800-61 (Rev. 2) • NIST CSF: DE.AE-1 -5, PR.DS-6, RS.AN-1, RS.AN-4, and PR.DS-8 • OMB M-20-04 • OMB M-21-31 • OMB M-22-01 • OMB M-23-03 • CISA Cybersecurity Incident Response Playbooks • CIS Top 18 Security Controls: Control 17 • US-CERT Federal Incident Notification Guidelines • FY 2023 CIO FISMA Metrics: 3.1, 10.4, 10.5, and 10.6	Core Metric	The organization has not defined and communicated its policies, procedures, and processes for incident detection and analysis. In addition, the organization has not defined a common threat vector taxonomy for classifying incidents and its processes for detecting, analyzing, and prioritizing incidents.	The organization has defined and communicated its policies, procedures, and processes for incident detection and analysis. In addition, the organization has defined a common threat vector taxonomy and developed handling procedures for specific types of incidents, as appropriate. In addition, the organization has defined its processes and supporting technologies for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed, and for prioritizing incidents.	The organization consistently implements its policies, procedures, and processes for incident detection and analysis. In addition, the organization consistently uses its threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization. In addition, the organization consistently implements, and analyzes precursors and indicators generated by, for example, the following technologies: intrusion detection/prevention, security information and event management (SIEM), antivirus and antispam software, and file integrity checking software. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident detection policies and procedures and making updates as necessary. In addition, the organization is meeting logging requirements at maturity EL1 (basic), in accordance with M-21-31.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident detection and analysis policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. The organization uses profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents. Examples of profiling include running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. Through profiling techniques, the organization maintains a comprehensive baseline of network operations and expected data flows for users and systems. In addition, the organization is meeting logging requirements at maturity EL2 (intermediate), in accordance with M-21-31.	The organization is making demonstrated progress towards implementing EL3's (advanced) requirements for its logging capabilities.

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
55. How mature are the organization's processes for incident handling?	• NIST SP 800-53 (Rev. 5): IR-4 • NIST SP 800-61 (Rev. 2) • NIST IR 8374 • NIST CSF: RS.MI-1 and RS.MI-2 • OMB M-21-31 • OMB M-23-03 • CISA Cybersecurity Incident Response Playbooks • FY 2023 CIO FISMA Metrics: 10.4, 10.5, and 10.6	Core Metric	The organization has not defined its policies, procedures, and processes for incident handling to include containment strategies for various types of major incidents, eradication activities to eliminate components of an incident and mitigate any vulnerabilities that were exploited, and recovery of systems.	The organization has defined its policies, procedures, and processes for incident handling to include containment strategies for each key incident type. In developing its strategies, the organization takes into consideration: the potential damage to and theft of resources, the need for evidence preservation, service availability, time and resources needed to implement the strategy, effectiveness of the strategy, and duration of the solution. In addition, the organization has defined its processes to eradicate components of an incident, mitigate any vulnerabilities that were exploited, and recover system operations.	The organization consistently implements its incident handling policies, procedures, containment strategies, and incident eradication processes. In addition, the organization consistently implements processes to remediate vulnerabilities that may have been exploited on the target system(s) and recovers system operations. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident handling policies and procedures and making updates as necessary.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident handling policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. The organization manages and measures the impact of successful incidents and can quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability.	The organization uses dynamic reconfiguration (e.g., changes to router rules, access control lists, and filter rules for firewalls and gateways) to stop attacks, misdirect attackers, and to isolate components of systems.
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 • NIST SP 800-53 (Rev. 5): IR-6 • NIST CSF: RS.CO-2 through RS.CO-5 • OMB M-20-04 • US-CERT Federal Incident Notification Guidelines • PPD-41 • DHS Cyber Incident Reporting Unified Message	FY24	The organization has not defined its policies, procedures, and processes to share incident response information with individuals with significant security responsibilities or its processes for reporting security incidents, including major incidents, to US-CERT and other stakeholders (e.g., Congress and the Inspector General, as applicable) in a timely manner.	The organization has defined its policies, procedures, and processes to report suspected security incidents to the organization's incident response capability within organization defined timeframes. In addition, the organization has defined its processes for reporting security incident information, including for major incidents, to US-CERT, law enforcement, the Congress and the Office of Inspector General, as appropriate.	The organization consistently shares information on incident activities with internal stakeholders. The organization ensures that security incidents are reported to US-CERT, law enforcement, the Office of Inspector General, and the Congress (for major incidents) in a timely manner. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident reporting policies and procedures and making updates as necessary.	Incident response metrics are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization receives, retains, uses, and disseminates cyber threat indicators in accordance with the Cybersecurity Information Sharing Act of 2015.

RECOVER FUNCTION AREA

Contingency Planning

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
61. To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts?	• NIST SP 800-34 (Rev. 1): Section 3.2 • NIST SP 800-53 (Rev. 5): CP-2 and RA-9 • NIST IR 8179 • NIST IR 8286 • NIST IR 8286D • NIST CSF: ID.RA-4 • FIPS 199 • FCD-1 • FCD-2 • OMB M-19-03	Core Metric	The organization has not defined its policies, procedures, and processes for conducting organizational and system-level BIAs and for incorporating the results into strategy and plan development efforts.	The organization has defined its policies, procedures, and processes for conducting organizational and system-level BIAs and for incorporating the results into strategy and plan development efforts.	The organization consistently incorporates the results of organizational and system level BIAs into strategy and plan development efforts. System level BIAs are integrated with the organizational level BIA and include: • Characterization of all system components • Determination of missions/business processes and recovery criticality • Identification of resource requirements • Identification of recovery priorities for system resources. The results of the BIA are consistently used to determine contingency planning requirements and priorities, including mission essential functions/high value assets.	The organization ensures that the results of organizational and system level BIAs are integrated with enterprise risk management processes, for consistently evaluating, recording, and monitoring the criticality and sensitivity of enterprise assets. As appropriate, the organization uses the results of its BIA in conjunction with its risk register to calculate potential losses and inform senior level decision making.	The organization integrates its BIA and asset management processes to improve risk identification, accurate exposure consideration (based on realistic calculations of harmful impacts), and effective risk response.
62. To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans?	• NIST SP 800-34 • NIST SP 800-53 (Rev. 5) CP-2 • NIST CSF: PR.IP-9 • FY 2023 CIO FISMA Metrics: 10.1.2, 10.2, and 10.3 • OMB M-19-03	FY24	The organization has not defined its policies, procedures, and processes for information system contingency plan (ISCP) development and maintenance. In addition, the organization has not developed templates to guide plan development; and system contingency plans are developed in an ad-hoc manner with limited integration with other continuity plans.	The organization has defined its policies, procedure, and processes for information system contingency plan development, maintenance, and integration with other continuity areas. The policies, procedures, and processes for ISCP include the following phases: activation and notification, recovery, and reconstitution.	Information system contingency plans are consistently developed and implemented for systems, as appropriate, and include organizational and system level considerations for the following phases: activation and notification, recovery, and reconstitution. In addition, system level contingency planning development/maintenance activities are integrated with other continuity areas including organization and	The organization can integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency, as appropriate to deliver persistent situational awareness across the organization.	Information system contingency planning activities are fully integrated with the enterprise risk management program, strategic planning processes, capital allocation/budgeting, and other mission/business areas and embedded into daily decision making across the organization.

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
					business process continuity, disaster recovery planning, incident management, insider threat implementation plan (as appropriate), and occupant emergency plans.	The organization coordinates the development of ISCP's with the contingency plans of external service providers.	
63. To what extent does the organization perform tests/exercises of its information system contingency planning processes?	• NIST SP 800-34 • NIST SP 800-53 (Rev. 5): CP-3 and CP-4 • NIST CSF: ID.SC-5 and PR.IP-10 • CIS Top 18 Security Controls: Control 11	Core Metric	The organization has not defined its policies, procedures, and processes for information system contingency plan testing/exercises. ISCP tests are performed in an ad-hoc, reactive manner.	Policies, procedures, and processes for information system contingency plan testing and exercises have been defined and include, as applicable, notification procedures, system recovery on an alternate platform from backup media, internal and external connectivity, system performance using alternate equipment, restoration of normal procedures, and coordination with other business areas/continuity plans, and tabletop and functional exercises.	Information system contingency plan testing and exercises are consistently implemented. ISCP testing and exercises are integrated, to the extent practicable, with testing of related plans, such as incident response plan/COOP/BCP.	The organization employs automated mechanisms to test system contingency plans more thoroughly and effectively. In addition, the organization coordinates plan testing with external stakeholders (e.g., ICT supply chain partners/providers), as appropriate.	Based on risk, the organization performs a full recovery and reconstitution of systems to a known state. In addition, the organization proactively employs [organization defined mechanisms] to disrupt or adversely affect the system or system component and test the effectiveness of contingency planning processes.
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 800-34: Sections 3.4.1 through 3.4.3 • NIST SP 800-53 (Rev. 5): CP-6, CP-7, CP-8, CP-9, and CP-10 • NIST SP 800-209 • NIST CSF: PR.IP-4 • FCD-1 • FY 2023 CIO FISMA Metrics: 10.3.1 and 10.3.2 • NIST Security Measures for EO-Critical Software Use: SM 2.5	FY24	The organization has not defined its policies, procedures, processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and redundant array of independent disks (RAID), as appropriate. Information system backup and storage is performed in an ad-hoc, reactive manner.	The organization has defined its policies, procedures, processes, strategies, and technologies for information system backup and storage, including use of alternate storage and processing sites and RAID, as appropriate. The organization has considered alternative approaches when developing its backup and storage strategies, including cost, environment (e.g., cloud model deployed), maximum downtimes, recovery priorities, and integration with other contingency plans.	The organization consistently implements its policies, procedures, processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and RAID, as appropriate. Alternate processing and storage sites are chosen based upon risk assessments that ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized. In addition, the organization ensures that these sites and are not subject to the same risks as the primary site. Furthermore, the organization ensures that alternate processing and storage facilities are	The organization ensures that its information system backup and storage processes, including use of alternate storage and processing sties, and related supply chain controls, are assessed, as appropriate, as part of its continuous monitoring program. As part of its continuous monitoring processes, the organization demonstrates that its system backup and storage and alternate storage and processing sites are configured to facilitate recovery operations in accordance with recovery time and recover point objectives.	The organization takes appropriate steps to protect against infection or other compromise of its backup data. Further, on a near real-time basis, for sensitive data and EO-critical software, the organization maintains an up-to-date recovery catalog for each backup that records which anti-malware tool the backups have been scanned with. In addition, for sensitive data, the organization periodically scans a subset of past backups with current anti-malware tools to identify poisoned backups.

Metric Number and Question	Criteria	Review Cycle	Maturity Level: Ad Hoc	Maturity Level: Defined	Maturity Level: Consistently Implemented	Maturity Level: Managed and Measurable	Maturity Level: Optimized
					configured with information security safeguards equivalent to those of the primary site, including applicable ICT supply chain controls. Furthermore, backups of information at the user- and system-levels are consistently performed, and the confidentiality, integrity, and availability of this information is maintained.		