FY 2024
Inspector General
Federal Information
Security Modernization Act of 2014
(FISMA) Metrics
Evaluator's Guide

VERSION 4.0
APRIL 30, 2024

Contents

Introduction

Summary
To promote consistency in Inspectors General (IG) annual evaluations performed under the Federal Information Security Modernization Act of 2014 (FISMA), the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in coordination with the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and the Federal Chief Information Officers and Chief Information Security Officers (CISO) councils are providing this evaluation guide for IGs to use in their FY 2024 FISMA evaluations.

The guide provides a baseline of suggested sources of evidence and test steps/objectives that can be used by IGs as part of their FISMA evaluations. The guide also includes suggested types of analysis that IGs may perform to assess capabilities in given areas. The guide should be considered for suggested source evidence that IGs may request to answer a metric. The guide should not be considered as an all-inclusive list of source evidence or test methods to reach the various maturity levels within metrics and domains. The test methods are not all inclusive and may not apply in all situations. Additional sources such as penetration testing results may be effective sources of evidence for select metrics.

The "Assessor's Best Practices" section has replaced the "Additional Notes" section this year. This section now breaks out the four maturity levels beyond Ad-Hoc to provide the assessor specific evaluation steps to consider for consistent assessment and testing. The steps provided are ones that have been used by experienced assessors and align to the maturity level and criteria for success.

The guide is a companion document to the FY 2023-2024 IG FISMA metrics[1] and provides guidance to IGs to assist in their FISMA evaluations.

Determining Effectiveness with IG Metrics
IGs are required to assess the effectiveness of information security programs on a maturity model spectrum, in which the foundational levels ensure that agencies develop sound policies and procedures, and at the advanced levels capture the extent that agencies institutionalize those policies and procedures. The five maturity model levels are ad hoc (level 1), defined (level 2), consistently implemented (level 3), managed and measurable (level 4), and optimized (level 5). Within the context of the maturity model, OMB believes that achieving managed and measurable (level 4) or above represents an effective level of security. The National Institute of Standards and Technology (NIST) provides additional guidance for determining the effectiveness of security controls.[2] IGs should consider both their and the agency's assessment of unique missions, resources, and challenges when determining information security program effectiveness. IGs have the discretion to determine whether an agency is effective in each of the Cybersecurity Framework Function (such as identify, protect, detect, respond, and recover) and whether the agency's overall information security program is effective based on the results of the determinations of effectiveness in each function and the overall assessment. Therefore, an IG has the discretion to determine that an agency's information security program is effective even if the agency does not achieve managed and measurable (level 4). Some agencies might uniquely

[1] Final FY 2023 - 2024 IG FISMA Reporting Metrics v1.1 (cisa.gov)
[2] NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations

meet these maturity levels, acknowledging the diverse nature of federal agencies' missions and resources.

Reflecting OMB's shift in emphasis away from compliance in favor of risk management-based security outcomes, IGs are encouraged to evaluate the IG metrics based on the risk tolerance and threat model of their agency and to focus on the practical security impact of weak control implementations, rather than strictly evaluating from a view of compliance or the mere presence or absence of controls. In response to the threat environment and technology ecosystem which continue to evolve and change at a faster pace each year, OMB implemented a new framework regarding the timing and focus of assessments in FY 2022. The goal of this new framework was to provide a more flexible but continued focus on annual assessments for the federal community. This effort yielded two distinct groups of metrics: **Core and Supplemental**.

Core Metrics
There are 20 core metrics. The core metrics are assessed annually by the IGs and represent a combination of Administration priorities, high impact security processes, and essential functions necessary to determine security program effectiveness.

Supplemental Metrics
Supplemental metrics are metrics that are assessed at least once every two years, and represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness. For FY 2023 FISMA, there were 20 supplemental metrics to review. FY 2024 includes 17 supplemental metrics to review.

Terms
The terms "*organization*" and "*enterprise*" are often used interchangeably. However, for the purposes of this document, an organization is defined as an entity of any size, complexity, or positioning within a larger organizational structure (e.g., a federal agency or department). An enterprise is an organization by this definition, but it exists at the top level of the hierarchy where individual senior leaders have unique risk management responsibilities (e.g., federal agency or department). In terms of cybersecurity risk management (CSRM), most responsibilities tend to be carried out by individual organizations within an enterprise. In contrast, the responsibility for tracking key enterprise risks and their impacts on objectives is held by top-level corporate officers and board members who have fiduciary and reporting duties not performed anywhere else in the enterprise.[3]

The terms "auditor", "assessor", "evaluator", "IG", and "OIG" are often used interchangeably. It is understood that the individuals performing the FISMA Metric reviews will vary from agency to agency. It is also understood that some agencies have chosen to outsource the evaluation to contracted service providers.

Recommendations Guidance
Although assessors have autonomy over what they feel is an appropriate recommendation for their organization, this section provides some general guidance for consideration to make recommendations more consistent and effective across the Federal government.

[3] NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Management

How should a recommendation be written?
To facilitate a steady progression through the maturity model,[4] recommendations should be written from the perspective of what level the organization is at for the metric, and what it would take to progress to the next level. As a general best practice, broad recommendations should be avoided. Recommendations should be focused on specific actions to address the root cause and lead the agency to that next maturity level. It may require several recommendations to get that metric to the next level, however this provides the agency with specific guidance and the opportunity to make steady and visible progress. This approach would also allow the assessors to follow-up on agency actions taken as part of their recommendation follow-up processes and/or the next FISMA evaluation. It is a matter of opinion, however generally a higher quantity of specific recommendations is preferable over fewer broad recommendations.

How should agencies consider plans of action and milestone (POA&M)?
As part of the data collection process, it is recommended that assessors collect and consider open POA&Ms that the organization has self-identified (or other means, such as past GAO or OIG reports, or assessment and authorization reviews) as issues they are working to resolve. As a best practice, assessors should avoid issuing recommendations that the organization is aware of and actively working to resolve. To re-emphasize the open POA&M assessors should consider referencing them in the narrative write up. Another potential approach would be to issue an "Opportunity for Improvement" (OFI) or an "Item for Management's Consideration" (IMC) to state that the organization should prioritize the POA&M in order to continue to mature the metric, domain, or program. OFIs and IMCs would be an "unofficial" recommendation that the assessor can issue in the report that does not get tracked in monthly reports and semi-annual reports (SAR), but rather just goes on record to emphasize the issue. OFIs and IMCs could become recommendations over time (generally 1-2 years) if the POA&Ms or OFIs and IMCs are not timely resolved. Additionally, POA&M process effectiveness in metric 8 could also be impacted by the inability to implement POA&Ms.

How should OIGs and agencies agree and keep recommendation remediation plans up-to-date?
Ordinarily, OIGs and Agency officials review and collaborate on recommendations to come to a management decision. This is either done through the agency's official comments to the report or during recommendation follow-up. During the management decision process it is critical that all parties are clear and agree upon the agency's planned corrective action. This is the time to ensure that the planned corrective action meets the intent of the recommendation and the selected NIST Special Publication (SP) 800-53 controls (or other applicable criteria). A healthy back and forth conversation to come to an agreed upon planned corrective action will ensure that the implemented corrective action also align. Occasionally planned corrective actions may change due to recency and relevancy (time to fix, resources, change in technology, etc.) and in these cases it's recommended that agency officials renegotiate the new planned corrective actions with OIG officials to develop an updated, agreed upon management decision.

What should OIGs and agencies do if a recommendation is overcome by events (OBE)?
Technology and cyberspace are constantly *and rapidly* changing. A recommendation made today may quickly be OBE and no longer be feasible. Rather than leaving a recommendation

[4] FY 2023-2024 Inspector General FISMA Reporting Metrics, pages 6-7

open and trying to figure out how to address it, or simply closing it, OIGs should consider closing the recommendation with a status of "Unresolved – Closed", which records the fact that the agency was not able to address the issue. Then, if appropriate, an updated and refocused recommendation should be issued and go through the MD process to help facilitate the agency's efforts to meet the OIG's original intent.

Conclusion

The tables below show the IG metrics for the entire FY22-24 cycle, including updates for the FY 2024 IG evaluation period. These metrics were selected for their applicability to critical efforts emanating from Executive Order 14028 and OMB M-24-04.

Risk Management

1. To what extent does the organization maintain a comprehensive and accurate ***inventory of its information systems*** (including cloud systems, public facing websites, and third-party systems), and system interconnections?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53, Rev. 5: CA-3, PM-5, and CM-8 • NIST Cybersecurity Framework (CSF) ID.AM-1 – 4 • NIST SP 800-37, Rev. 2 • OMB A-130 • OMB M-24-04 • FY 2024 CIO FISMA Metrics	Core	**Ad Hoc** 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.	
		Defined 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.	• Directives, policies, procedures, standards, strategies, and/or standards associated with the system registration and inventory process; • System interconnect inventory processes and procedures; • Information Security Program policies and procedures; • Ongoing authorization policies and procedures.

Criteria	Review	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented 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.	• Organization-wide information systems inventory, including contractor operated information systems, cloud systems, public facing websites, and third-party systems; • Program/division-level information systems inventories; • Data Flow policies/procedures (to validate the completeness of the approved system inventory); • Enterprise Architecture references (to validate the completeness of the approved system inventory); • Final Interconnection Security Agreements (ISAs)/MOUs/MOAs/etc.) to validate the completeness of the approved system inventory; • List of non.gov fully qualified domain names (FQDN) in use by the agency; • Evidence that agencies provided all non.gov FQDNs used to CISA and GSA (e.g., dashboard reports, email messages, etc.); • CISA provided data about internet-accessible assets; • The results of any website scanning services performed by an independent third-party (e.g., OIGs, GSA, etc.) to assess the completeness of the approved system inventory[5]; • Change control requests; • FedRAMP PMO communications; • EA Documentation; • Web app domain registry information.

Criteria	Review	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable The organization ensures that the information systems included in its inventory are subject to the monitoring processes defined within the organization's ISCM strategy.	• ISCM strategy/plan; • Continuous monitoring reports/dashboards; • CDM artifacts.
		Optimized 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.	• Dashboard reports/observations; • Hardware and software component inventories; • Asset database reports; • Evidence the reports and alerts which indicate changes to the inventory are updated in real-time.

[5] https://digital.gov/guides/site-scanning/

Assessor Best Practices
Defined: Assessors should determine whether the agency's system inventory management policies/procedures/processes address the addition of new systems (registration) and the retirement of old systems. Assessors should assess these policies and procedures to determine whether system boundary considerations (e.g., bundling, mobile devices, cloud deployments, etc.) are outlined for inventorying. These policy documents should also outline processes associated with registering information systems and maintaining the organization's information system inventory. Artifacts that support maintaining a current system inventory include those gathered from FISMA compliance tools (e.g., Cybersecurity Assessment and Management (CSAM)) and other tools that may be deployed to capture component inventory information, infrastructure configuration management processes, SDLC processes, EA processes, and may be captured in a general Information Security Program policy. **Consistently implemented:** As part of the analysis performed by the assessor for public facing web applications, utilize open-source tools/information (e.g., digitaldashboard.gov) to identify the agencies subdomains and related services and compare against the inventory of information maintained by the agency for completeness and accuracy. The assessor should determine if the inventory was approved and completed and maintained in accordance with agency policies and procedures. Determine if the system level inventories reconcile to the organization-wide system inventory. Evidence collected should demonstrate that the agency used the GSA list of non .gov agency websites to reconcile against its approved inventory of webapps/websites sites and performed appropriate actions to update and responded to newly discovered websites/apps. Assessors should use the CISA provided data about agencies' internet-accessible assets data to evaluate the completeness of the public web app inventory. Assessors may also consider reviewing change control ticket, FedRAMP PMO communications, and EA documentation to confirm the completeness of the approved system inventory (including those hosted on-prem). Assessors should also consider reviewing FISMA compliance tools (e.g., CSAM) records, EA documentation, SDLC/change control records, etc. to ensure the accuracy and completeness of the inventory. Ensure to verify IT assets that are not regularly connected to the agencies' networks. For examples, they can be: • New IT equipment that have not been put into service • Older IT equipment that are not being used, whether decommissioned or not • IT loaner equipment Agencies that use tools like CSAM as the source of their official IT inventory list do not track the above examples of IT assets since CSAM drops devices that are not connected for some time. **Managed and measurable:** Assessors should reconcile the list of systems in the organization's approved inventory to ensure those systems are included in the organization's continuous monitoring processes to identify any variances. CDM artifacts, change control tickets, FedRAMP PMO communications, Web App domain registry information, and EA documentation should all be reflected in the system inventory. **Optimized:** Sample select systems from the organization's approved inventory to determine whether the agency can automatically identify system hardware/software components and supply chain vendors and make updates in a near-real time fashion. Assessors should also ensure that security tools (e.g., IDS, IPS, NAC etc.) and related configuration management solutions (e.g., CMDBs) are updated in real time as new systems are implemented.

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?			
Criteria	**Review Cycle**	**Maturity Level**	**Suggested Standard Source Evidence**
• NIST SP 800-37, Rev. 2: Task P-10 and P-16 • NIST SP 800-53 Rev. 5: CA-7 and CM-8 • NIST SP 800-137 • NIST 800-207 • NIST 1800-5 • NIST IR 8011	Core	**Ad Hoc** 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 with the detailed information necessary for tracking and reporting.	

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• Federal Enterprise Architecture (FEA) Framework, v2 • EO 14028, Section 3 • OMB M-24-04 • OMB M-22-09, Federal Zero Trust Strategy, Section B • CSF: ID.AM-1 • CISA Cybersecurity & Incident Response Playbooks • CIS Top 18 Security Controls: Control 1 • BOD 23-01 • BOD 23-01 Implementation Guidance • FY 2024 CIO FISMA Metrics		**Defined** 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.	• Policies and procedures (and related guidance) for hardware asset inventory management • Hardware naming standards/standard taxonomy document • ISCM policies and procedures • Network Access Control policies and procedures • BYOD policies and procedures • End user computing device inventory standards • Enterprise Architecture bricks • Scanning policies (including automated asset discovery policies) and procedures • Information system component policies and procedures • Control baselines

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented 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.	• Authorized hardware inventory (which includes, but not limited to, applications (COTS and GOTS), servers, workstations, input and output devices, network devices, and mobile devices (GFE and non-GFE in an approved BYOD environment); • Listing of the hardware purchases (the inventory specifications should include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location); • Agency SSPs; • Information System Component Inventories; • Continuous monitoring reports (e.g., vulnerability scanning reports, Splunk logs/reports, SCCM reports, etc.); • Enterprise Architecture documents; • Inventory dashboards; • Firewall configurations/logs; • Configuration Management Database dashboards/reports; • IT asset management (ITAM) solution dashboard/reports (e.g., ServiceNow, CSAM, Forescout, CounterACT, BigFix, etc.); • DHS CDM dashboards/reports which reconcile 80% to agency records (e.g., scanning results/ITAM reports); • Scans configured to cover all agency networks and IP ranges (to validate completeness).

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable 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.	• Continuous monitoring reports/dashboards (e.g., CDM, PowerBI, Splunk, etc.); • ISCM reports; • FISMA compliance tool reports (such as CSAM and RSAM); • Mobile device management implementation.
		Optimized 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.	• ITAM/hardware asset management reports; • Mobile Device Management solution configuration or reports; • Continuous monitoring dashboards or reports; • Enterprise Architecture documentation or reports; • Examples of security alerts resulting from unauthorized hardware being placed on the network.

Assessor Best Practices
Defined: Assessors should determine whether the organization's policies and procedures define the requirements and processes for IT hardware asset management, including the standard data elements/taxonomy required to be recorded, reported, and accurately maintained. Assessors should also ensure that the organization is not double counting system components (please see CM-8 for more information on this). These policies and procedures should also include how automated asset discovery is planned or being used to inventorying IT hardware assets. In addition, assessors should verify that the agency has defined how the organization maintains an up-to-date inventory of the hardware assets connected to its network, and the organization's processes to control which hardware assets (including BYOD mobile devices) can connect to its network. These may be defined in SOPs and control baselines. Assessors should also ensure that these policies and procedures include the DHS BOD 23-01 requirements, such as automated asset discovery frequencies (minimum at least every 7 days), includes (at least) the entire IPv4 space used by the organization, collecting appropriate CISA approvals, and a requirement to perform automated asset recovery upon CISA demand within 72 hours. **Consistently implemented:** Determine if the agency can reconcile its hardware asset inventory to the assets live on its network (i.e., through automated hardware asset discovery. Please note, any sample should include assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. The sample should also be inclusive of all assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. In addition, the organization has made sufficient progress towards reporting at least 80% of its Government Furnished Equipment (GFE) through the DHS CDM program (e.g., if 80% is not achieved a reasonable plan to reach this goal has been documented and approved by the appropriate stakeholders). Assessors should also validate the completeness of the hardware inventory by reconciling the Information System Component Inventories against the hardware inventory. Assessors should also consider reviewing firewall/configuration logs to identify unauthorized hardware. **Managed and measurable:** Sample select systems and verify that hardware assets are subject to the organization's continuous monitoring processes through an organization-wide hardware asset management capability. Verify that quantifiable metrics are used to manage and measure the implementation of the organization's ISCM processes for the hardware assets sampled. The organization should also ensure that unauthorized assets are removed from the network, quarantined, and the inventory is updated in a timely manner. The organization uses port level access controls to control which hardware devices can authenticate to the network. **Optimized:** Determine whether the organization uses automated tools for ITAM/hardware asset management and dashboarding (such as ServiceNow, CSAM, Forescout, CounterACT, BigFix, MaaS360, CDM, PowerBI, Splunk, etc.) For sampled systems, determine whether the hardware asset information in the automated tools is accurate, complete, reporting in real time, and integrated (either procedurally or automatically) into the organization's process to update its enterprise architecture.

3. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?			
Criteria	**Review Cycle**	**Maturity Level**	**Suggested Standard Source Evidence**
• NIST SP 800-37, Rev. 2: Task P-10 • NIST SP 800-53 Rev. 5: CA-7, CM-8, CM-10 and CM-11 • NIST SP 800-137 • NIST 800-207, Section 7.3 • NIST 1800-5	Core	**Ad Hoc** 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 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.	

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence

• NIST IR 8011
• NIST Security Measures for EO-Critical Software Use
• CSF: ID.AM-2
• FEA Framework
• EO 14028, Section 4
• OMB M-21-30
• OMB M-22-09
• CISA Cybersecurity & Incident Response Playbooks
• FY 2024 CIO FISMA Metrics
• CIS Top 18 Security Controls v.8: Control 2
		Defined
		The organization has defined policies, procedures, and processes for using standard data 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.
			• Policies and procedures (and related guidance) for software/license/asset management;
			• Software naming standards/standard taxonomy document;
			• Standard software images for devices;
			• BYOD policies and procedures (e.g., mobile app rules);
			• Enterprise Architecture bricks;
			• Scanning policies and procedures;
			• Information system component policies and procedures;
			• Change control policies and procedures;
			• ISCM policies and procedures;
			• SOPs for software and application:
			  ○ use of automation to maintain inventories
			  ○ protecting against unauthorized software
			  ○ ensuring licensing conformance, restrictions, expiration, etc.
			  ○ managing licenses utilization.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented The organization consistently uses its standard data 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 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.	• Authorized software inventory which includes EO-critical software; • Agency SSPs; • Change control tickets; • Information System Component Inventories (to validate the completeness of the software inventory by reconciling against the software inventory); • Enterprise Architecture documents; • Inventory dashboards; • Firewall configurations/logs; • CMDB dashboards/reports; • Software license inventory listing, • Whitelisting/blacklisting tool (e.g., Applocker) system configurations, etc.)

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable The organization ensures that the software assets, including EO-critical software and mobile applications as 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).	• Authorized software inventory; • Scans that gather device profiles and update information on software assets/licenses (to validate completeness); • Continuous monitoring reports/dashboards (e.g., vulnerability scanning reports, SIEM logs/reports, SCCM/Puppet reports, etc.) which list the software assets (including EO-critical software and mobile applications); • ISCM strategy; • Whitelisting/blacklisting tool (e.g., Applocker) system configurations; • MaaS configurations, reports. dashboards, etc.; • Evidence that unauthorized software is blocked.
		Optimized The organization employs automation to track the life cycle of the organization's software assets (and their 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.	• Scanning and alert results, which provides updates for the solution used to track software throughout its lifecycle on a near-real time basis, or other examples of security alerts resulting from unauthorized hardware/software being placed on the network; • Network scanning reports; • MaaS configurations, reports, dashboards, etc.; • EA documentation; • Software inventory.

Assessor Best Practices
Defined: Assessors should determine whether the organization's policies and procedures define the requirements and processes for software asset management, including the standard data elements/taxonomy required to be recorded, reported, and maintained. In addition, Assessors should verify that the agency has defined its processes for software license management (including for mobile applications), and ensure these processes include roles and responsibilities. Assessors should also verify that processes are documented which outline how the organization ensures the completeness of the software inventory, including how the organization validates all EO-critical software and mobile applications are included in the software inventory. **Consistently implemented:** The agency can reconcile its software asset inventory to the assets live on its network (including EO-critical software and mobile applications). Assessors should verify that unauthorized software is removed and the inventory is updated in a timely manner (CIS Controls V. 8, #2.3). In addition, at level 3, the agency should be able to identify unlicensed software from running on the network and restrict licensed software to authorized users/systems. Also, assessors should review the types of EO-critical software defined by NIST and validate that this software types listed are captured in the approved software inventory and that the organization is following its defined processes to validate the completeness of the software inventory. The software inventory should also include all platforms running EO-critical software. Assessors also may also reconcile the Information System Component Inventories to the software inventory to validate the completeness of the software inventory. **Managed and measurable:** The agency has deployed application blacklist, whitelist, or cryptographic containerization technology on mobile devices, as appropriate, to ensure that only authorized software executes, and all unauthorized software is blocked from executing. The scope of the organization's ISCM program include EO-critical software. The organization's allow listing technology ensures that only authorized software libraries may load into a system process. **Optimized:** Assessors should obtain evidence [ex. network scanning reports designed to identify all instances of software, including EO-critical software and mobile applications, (and their associated licenses) executing on the organization's network(s), and software installation request/ project request authorizations] to ensure that the software executing in the organization's network(s) is identified and authorized.

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?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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 • OMB M-19-03 • FY 2024 CIO FISMA Metrics	FY2024	**Ad Hoc** 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.	
		Defined 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.	• Information classification standard and related policies and procedures; • Policy on categorization of information systems; • System/Information impact classification worksheets; • Data dictionaries. • Policies, procedures, and processes for controls allocation, selection and tailoring.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented 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.	• Security risk documentation (i.e., SSPs, categorization documents, HVA documents, system-level categorization sheets, etc.); • Approved organization-wide information systems inventory; • Identification of mission essential systems and high value assets (HVAs). • Evidence for compliance with OMB M-19-03 and inputs for the HVA identification.
		Managed and Measurable 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.	• Prioritization of HVAs and activities. • Agency's POA&M policy and process • BIA • Agency's capital planning and investment control process. • Agency's prioritized plans to address HVA assessment findings
		Optimized The organization uses impact-level prioritization for additional granularity, and cybersecurity framework profiles, as appropriate, to support risk-based decision-making.	• Cybersecurity Framework profiles

Assessor Best Practices
Defined: Evaluate agency information security policies and procedures to determine if they define how the organization categories and communicates the importance and priority of its information systems. Furthermore, IG evaluators should determine whether the agency's policies and procedures in this area incorporate HVA related considerations, such as how HVA's are identified, prioritized, and secured. Furthermore, IG evaluators should determine whether the agency's information security policies, procedures, and/or control baselines have been updated to incorporate HVA considerations. For example, evaluate POA&M policies and procedures to determine whether HVA requirements have been established to determine if POA&M items are prioritized or validated/reviewed on a more frequent basis than non-HVAs. Evaluate ISCM policies and procedures to determine if HVAs are subject to more rigorous review processes. **Consistently Implemented:** IG evaluators should sample select systems and supporting documentation (SSP, system classification worksheets, BIA, data dictionaries etc.) to determine whether the categorization of select systems considers all relevant information types. The agency should demonstrate that system classifications take into consideration and are consistent with the importance/priority levels of the organization's mission and business functions (BIA). Determine if the agency has identified and communicated its high-value assets to stakeholders and established an HVA governance structure in accordance with OMB M 19-03. Determine whether relevant inputs were considered as part of the agency's identification of HVAs (e.g., business impact analysis, ERM, COOP). **Managed and measurable:** Determine whether the agency has implemented the methodology provided by DHS to prioritize HVAs and associated HVA activities. Furthermore, evaluate agency budget/CPIC processes to determine whether the HVA governance structure is working with OMB and DHS to appropriately allocate agency resources to HVAs and to ensure effective protection of HVAs. Determine whether implementation of HVA specific policy/procedural requirements/baselines are resourced/planned for and implemented, as appropriate. **Optimized:** Determine if impact level prioritization is being utilized to further classify the importance/priority of systems and whether the agency has developed supporting control baselines. At the optimized level, the organization physically, and/or logically segregates HVA's.

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?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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 • OMB A-123 • OMB M-16-17 • OMB M-24-04 • NIST CSF: ID RM-1 – ID.RM-3	Core	**Ad Hoc** The organization has not defined and communicated the policies, procedures and processes it utilizes 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	
		Defined The organization has defined and communicated the policies, procedures and processes it utilizes 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	• Enterprise Risk Management policies, procedures, and strategies; • Cybersecurity Risk Management policies, procedures, strategies; • Risk Assessment Policies and Procedures; • Ongoing Authorization policies and procedures; • System Categorization policies and procedures; • SDLC policies and procedures; • EA policies and procedures; • Risk Executive Council Charters/delegations of authority; • POA&M policies and procedures; • Organizational risk profiles; • SSPs.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented 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 utilizes the common vulnerability scoring system, or similar approach, to communicate the characteristics and severity of software vulnerabilities. Further, the organization utilizes 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.	• Risk Executive Council Charters; • Risk Council meeting minutes; • Organizational, Mission, and System-level Risk Assessments; • System Security Plans; • Security Assessment Reports; • System Risk Assessments; • System Categorization documents/worksheets; • Cybersecurity Framework profiles; • Risk registers/Cybersecurity risk registers (CSRRs); • Risk Detail Records (RDRs); • Risk heat maps; • POA&Ms; • Project plans/taskers; • Risk Council/steering committee meeting minutes; • Investment Review meeting minutes/taskers; • Lessons learned documents.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable The organization utilizes 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.	• Organization-wide risk assessment(s); • CSRR(s)s; • Risk Executive Council Charters; • Risk Council meeting minutes; • System-level risk assessments; • Privacy risk assessments; • Supply chain risk assessment results; • Information sharing agreements and/or MOUs; • Information system authorization procedures; • Risk management policies, procedures, and strategies, lessons learned; • Cybersecurity Framework profiles, periodic reviews of risk tolerance levels, etc.; • Business Impact Assessments.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Optimized 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 utilizes Cybersecurity Framework profiles to align cybersecurity outcomes with mission or business requirements, risk tolerance, and resources of the organization.	• Meeting minutes; • Email communications; • Cyber risk register updates; • System workflow results/interactions; • Investment/staffing documentation updates; • Strategic planning documentation updates; • Updates to the security program documentation - such as - updates to ISCM documentation, system security plans, system risk assessments; • Updates to security performance metrics; • Updates to system security plans; • Updates to Business Impact Assessment/COOP documents; • Enterprise risk profiles/documentation • Results of risk/loss scenario modeling exercises • NIST Cybersecurity Framework current/future state implementation documentation; etc.

Assessor Best Practices
Defined: The organization should demonstrate that it has established the overall context within which the organization functions and includes consideration of cybersecurity factors that affect the ability of an agency to meet its stated mission and objectives and this context should be formally documented in policies, procedures, strategy documents, or similar. These documents should also provide guidance on the form of the risk assessments conducted (including the scope, rigor, and formality of such assessments) and the method of reporting results. Assessors should obtain the organization's risk management policies, procedures, and strategy and ensure that the organization's risk appetite/tolerances are clearly defined and measurable. **Consistently Implemented:** Assessors should ensure that processes implemented, and results of risk assessments align with the defined organizational risk appetite/tolerances. Assessors should also ensure the organization's CSRRs clearly summarizes the organizations cyber risks

and provide adequate support (e.g., CVSS scores, CSF/CIS Top 18, compensating control evidence, etc.) for risk prioritization and proposed risk mitigation approaches.

Managed and measurable: Assessors collect and review the organization-wide risk assessment(s) and ensure that the results of the cyber risk registers and system level risk assessments are represented, and that the defined risk appetites/tolerances are regularly monitored/updated and maintained, and the effectiveness of risk responses are assessed. Assessors should also reconcile the information listed in the organization's CSRRs to the organization's RDRs and/or to other sources of risk information, such as incident response documentation, registry of system assets, security assessment reports, penetration test results, Business Impact Assessments (e.g., to identify the organization's mission essential functions/mission-critical systems), etc. to ensure that the information included in the CSRRs was aggregated, consistent across the documents, and normalized.

Optimized: Assessors should obtain artifacts evidencing that the organization utilizes Cybersecurity Framework profiles and enterprise risk profiles to align cybersecurity outcomes with mission or business requirements, and the risk appetite and tolerances of the organization. This includes confirming that the organization is maintaining a current financial valuation of its assets that require protection and/or the mission value of those assets (e.g., impact on mission capability/organizational reputation) and considers those valuations when planning remedial activities. Organizations may maintain this information in a business impact assessment along with risk/loss scenario modeling results which should act as inputs to the CSRR.

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 organization's supply chain?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-37 (Rev. 2): Task P-16 • NIST SP 800-39	FY2024	**Ad Hoc** 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 to introducing systems into its development environment.	

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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 • 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)		**Defined** The organization has defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture. 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).	• Related policies and procedures (including Architecture Review Board Charters); • System development lifecycle policies and procedures; • Open-source software policy; • IT architecture policy; • Desktop software approval procedures; • Enterprise Architecture policies; • Enterprise Architecture as-is and to-be states; • Agency mission and strategic plans.
		Consistently Implemented 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 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.	• Sample Security architecture/SIAs reviews of new acquired systems, hardware/software.
		Managed and Measurable 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 Communications Technology (ICT) supply chain and the organization's information systems.	• Sample security/enterprise architecture status reports; • Current and target enterprise architecture documents (highlighting the architecture changes resulting from hardware/software implementations).

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Optimized: 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 architectures to mitigate supply chain risks.	• Evidence of avoidance of the purchase of custom configurations; • Evidence of the use of a diverse set of suppliers; • Evidence of the use of approved vendor list with standing industry reputations. • Advanced technologies used for managing supply chain risk and demonstration and evidence of the capabilities of these technologies.

Assessor Best Practices
Defined: Verify that the organization has developed an organization-wide information security architecture. Ensure that development/maintenance of the information security architecture is coordinated with the Senior Agency Official for Privacy to ensure that security controls needed to support privacy requirements are identified and effectively implemented. Analyze the information security architecture to determine whether it describes the structure and behavior of the organization's security processes, information security systems, personnel, and organizational sub-units, showing their alignment with the organization's mission and strategic plans. Analyze the organization's system's development life cycle policies and procedures to determine whether the organization has defined system security engineering activities and tasks, as appropriate and in accordance with NIST 800-160v1. NIST 800-160v1 provides for flexibility on implementation of system security engineering principles and the intent at Defined is for IG evaluators to determine whether the organization, based on its missions, risks, threats, has integrated systems security engineering activities into its SDLC policies and procedures. **Consistently Implemented:** For sampled systems, verify that the information security architecture at the system level is consistent with and complements the more global, organization-wide information security architecture. This may be done by verifying that the use of security tools (e.g., for logging, monitoring, configuration) and automation at the system level is consistent with the overall security architecture. For sampled systems, select specific system security engineering activities and tasks defined in the organization's SDLC and verify that these were followed/have been implemented. This level of testing should be coordinated with other testing performed. For example, NIST 800-160, Rev 1 includes system security engineering activities and tasks related to acquisition of products and services. **Managed and measurable:** Determine whether the information security architecture is incorporated into and aligned with the organization's system's development lifecycle and enterprise architecture processes. Furthermore, the information security architecture should provide for traceability from the highest-level strategic goals and objectives of the organization (tier 1), through specific mission/business protection needs (tier 2), to specific information security solutions provided by people, processes, and technologies (tier 3). In addition, the organization has the

Managed and measurable: Determine whether the information security architecture is incorporated into and aligned with the organization's system's development lifecycle and enterprise architecture processes. Furthermore, the information security architecture should provide for traceability from the highest-level strategic goals and objectives of the organization (tier 1), through specific mission/business protection needs (tier 2), to specific information security solutions provided by people, processes, and technologies (tier 3). In addition, the organization has the ability to validate (though continuous monitoring processes) that its system security engineering and system life cycle processes are being effectively implemented across the agency and that deviations are identified and managed.

Optimized: Further, the organization implements supplier diversity concepts to ensure that [organization defined security safeguards] are obtained from different suppliers. An example could be the use of various suppliers for vulnerability scanning/configuration management at various stacks/levels (e.g., application, database, network/os).

7. To what extent have the ***roles and responsibilities*** of internal and external stakeholders involved in cybersecurity risk management processes been defined, communicated, and implemented, and appropriately resourced across the organization?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-37 (Rev. 2): Section 2.8 and Task P-1 • NIST SP 800-39: Sections 2.3.1, 2.3.2, and Appendix D • NIST SP 800-53 (Rev. 5): RA-1	FY2023	**Ad Hoc** Roles and responsibilities for cybersecurity risk management have not been defined and communicated across the organization. Further, the organization has not defined the relevant work roles for stages in the cybersecurity risk management process and which roles are responsible, accountable, consulted, or informed about various activities, as appropriate. In addition, the organization has not defined the relationships between cybersecurity risk management roles and those roles involved with enterprise risk management.	

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST CSF: ID.AM-6, ID.RM-1, and ID.GV-2 • NIST IR 8286: Section 3.1.1 • OMB A-123 • OMB M-19-03		**Defined** Roles and responsibilities of stakeholders involved in cybersecurity risk management processes have been defined and communicated across the organization. This includes the relevant work roles for stages in the cybersecurity risk management process and which roles are responsible, accountable, consulted, or informed about various activities, as appropriate. In addition, the organization has defined and clearly communicated the relationships between cybersecurity risk management roles and those roles involved with enterprise risk management.	• Information Security Program policy and procedures; • ERM policies, procedures, and strategies; • Risk Management Council/Risk Executive (function) Council Charter(s); • Organizational chart outlining all agency offices/lines of business; • Agency Strategic Plan; • Position descriptions, or other checklists, charters, or documents that include key information about senior leaders' delegated roles, responsibilities, and authorities.
		Consistently Implemented Individuals are consistently performing the cybersecurity risk management roles and responsibilities that have been defined across the organization. This includes roles and responsibilities related to integration with enterprise risk management processes, as appropriate.	• Executive Risk Council meeting minutes ; • Meeting minutes that include discussions about cyber risk/cyber risk management/maintaining cyber risk register; • CSRR(s) and CSRR updates; • Enterprise-level risk register; • Enterprise-level risk register updates; • Department-level risk registers (if applicable); • System-level risk assessment results.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement cybersecurity risk management activities and integrate those activities with enterprise risk management processes, as appropriate. Further, stakeholders involved in cybersecurity risk management are held accountable for carrying out their roles and responsibilities effectively.	• POA&Ms; • CSRR(s); • Enterprise-wide risk registers; • Enterprise risk profile (if separate from the Enterprise risk register; • Performance dashboards designed to monitor progress against stated metrics; • Performance appraisals for those with key roles in the ERM and cyber risk management processes; • Budget documents for business units involved in risk management; • Executive Risk Council meeting minutes; • Capital Planning and Investment Committee initiatives/minutes.
		Optimized The organization uses an integrated governance structure, in accordance with A-123, and associated review processes (e.g., ERM councils or IT investment review boards) to support the integration of roles and responsibilities for cybersecurity risk management and ERM.	• Enterprise-level risk register/risk profile; • Department/function-level risk registers; • Enterprise risk register which ties to department-level risk registers and CSRRs; • Evidence ERM meeting minutes, dashboards providing near real-time views of enterprise-wide and cyber risk.

Assessor Best Practices
Defined: Organizational risk management policies/strategies/charters should have clearly defined roles, responsibilities, delegated authorities, and accountability for individuals/committees that are part of the agency's ERM processes, including those at the enterprise, business/mission, and system levels, and this information should be communicated organization wide. Risk strategies should identify and tie to agency mission, programs, projects, etc. Senior officials for program operations and mission-support functions should also be included in the governance of the risk management function. Additionally, the organization's risk management policies/strategy should have clearly defined roles, responsibilities, and delegated authorities for individuals responsible for cyber risk management which is clearly integrated into the ERM function, and

accountability should be ensured (e.g., performance monitored) for those acting in risk management roles. Assessors should also ensure the objectives, scope, functions, organizational structure, and operating procedures (see the CFO Council Playbook on ERM) are clearly defined and include how cyber risk is integrated into the ERM process and how ERM stakeholders communicate with cyber risk stakeholders.

Consistently implemented: Assessors should confirm the organization's risk management policies/strategy was shared with the appropriate ERM stakeholders and those involved in cyber risk management as well as confirm those two groups are interacting according to organizational policy/charter requirements. Assessors should confirm the other questions in the Risk Management domain were met and consider those results when determining whether individuals are performing the roles and responsibilities, as required. Assessors should review meeting minutes and other artifacts (e.g., risk registers updates) to confirm the risk committees/councils are operating as designed.

Managed and measurable: The organization should demonstrate that resources (people, processes, and technologies) are allocated in a risk-based manner. For instance, at the system-level, the organization should be able to demonstrate that it is allocating resources first to the highest priority risks identified in its risk register and/or program-level POA&Ms. Similarly, at an enterprise level, the organization should be able to demonstrate that it is using its risk profile in resource allocation decisions (e.g., Capital Planning and Investment Committee initiatives). The organization should also demonstrate that individuals defined as having key risk management roles/responsibilities are being held accountable. This may be evidenced through the use of metrics for managing the completion and effectiveness of risk management activities. This may also be evidenced by inclusion of specific risk-management activities and objectives in performance review processes.

Optimized: The organization should have implemented an integrated governance structure that effectively directs and oversees the implementation of all the provisions of a robust process for risk management and internal control, in accordance with A-123 which includes ensuring that updates to legislation effecting cyber governance and the results of a major data breaches/cyber incidents are reflected in the appropriate risk registers/supporting documentation. This also required that the departmental risk registers and CSRRs are integrated into the ERM process in near real-time.

8. To what extent has the organization ensured that ***plans of action and milestones (POA&Ms)*** are used for effectively mitigating security weaknesses?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-37 (Rev. 2): Tasks A-6, R-3 • NIST SP 800-53 (Rev. 5): CA-5 and PM-4	FY2023	**Ad Hoc** Policies and procedures for the effective use of POA&Ms to mitigate security weaknesses have not been defined and communicated.	

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST CSF: ID.RA-6 • OMB M-14-04 • OMB M-19-03		**Defined** Policies and procedures for the effective use of POA&Ms have been defined and communicated. These policies and procedures address, at a minimum, the centralized tracking of security weaknesses, prioritization of remediation efforts, monitoring and maintenance, and independent validation of POA&M activities.	• Information security program policy and procedures; • POA&M policies and procedures; • Ongoing authorization policies and procedures; • ISCM policy, procedures, and strategies, etc.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented The organization consistently uses POA&Ms to effectively mitigate security weaknesses. The organization uses a prioritized and consistent approach to POA&Ms that considers: • Security categorizations • Security, privacy, and supply chain risk assessments • Specific control deficiencies and their criticality • Rationale for accepting certain deficiencies in controls • Required PPOA&M attributes, in accordance with OMB M-04-14 (e.g., severity and brief description of the weakness, remediation tasks and milestones for meeting those tasks, and estimated funding resources required to resolve the weakness) Further, the organization uses lessons learned in implementation to review and update its POA&M processes.	• System level POA&Ms/ POA&M dashboard reports (e.g., CSAM); • Enterprise-wide POA&Ms; • POA&M validation reports; • POA&M lessons learned; • System ATO's; • System risk assessments; • System Security Plans; • Security Assessment Reports; • Continuous monitoring reports; • Vulnerability scans; • Results of internal reviews; • Results of external review (e.g., GAO reports, IG reports, etc.); • Supply chain risk assessments; • Meeting minutes; • Change tickets for new hardware and software installations, or other remedial activity taken to address the POA&M; • Incident response taskers.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its POA&M activities and uses that information to make appropriate adjustments, as needed, to ensure that its risk posture is maintained.	• POAM status reports; • Scan results; • POA&M dashboards; • Results of internal POA&M validation reviews, evidence of the actions taken; • Enterprise and cyber risk profiles demonstrating the reduction in organizational/system risk as a result of taking POA&M actions.
		Optimized The organization employs automation to correlate security weaknesses amongst information systems and identify enterprise-wide trends and solutions in a near real-time basis. Further, processes are in place to identify and manage emerging risks, in addition to known security weaknesses.	• Evidence of POA&M automation (such as the use of a dashboard to view and correlate risks across the agency).

Assessor Best Practices
Defined: Assessors should collect and review organizational policies and procedures and ensure that the organization has defined and communicated how it tracks security weaknesses, prioritization of remediation efforts, maintenance, and independent validation of POA&M activities. **Consistently implemented:** Assessors should verify that system level POA&M's describe the actions planned to correct deficiencies identified during security controls assessments (including supply chain risk assessments) and continuous monitoring activities (See 800-37, Rev 2, Task A-6, "Discussion"). The POA&M should include tasks to be accomplished to mitigate deficiencies, resources required to accomplish the tasks, milestones established to meet the tasks, and the scheduled completion dates for the milestones and tasks (See 800-37, Rev 2, Task A-6, "Discussion"). The organization also should demonstrate that it has implemented a prioritized approach to risk mitigation across the enterprise. This prioritized approach, as noted in NIST SP 800-37, Rev. 2, Task P-6, ensures that POA&Ms are informed by the security categorization of the system; security, privacy, and supply chain risk assessments; the specific deficiencies in the controls; and the criticality of the control deficiencies. As such, at level 3, IG assessors should analyze POA&Ms for selected systems and determine if these types of considerations are factored into the prioritization of tasks to mitigate security weaknesses. Moreover, the organization should provide a rationale for accepting the risk associated with deficiencies identified in risk documentation (e.g., SSPs, SARs, system level risk assessments, supply chain risk assessments, incident response

taskers, etc.) not included in the POA&Ms. The organization should also demonstrate that POA&M remediation activities are independently verified and validated at a frequency outlined in supporting policies/procedures and include all attributes outline in OMB M-04-14 (e.g., severity and brief description of the weakness and estimated funding resources required to resolve the weakness) in the POA&Ms. The organization should also demonstrate that it performs periodic lessons learned to improve the POA&M process

Managed and measurable: The organization should implement metrics to manage and measure the effectiveness of risk reduction activities outlined in POA&Ms. Such measures should go beyond tracking of POA&M closure rates and POA&M closure timeliness and demonstrate how risk is being reduced. As such, the organization should have the ability to look across its system-level POA&Ms to identify common control weaknesses at the program level (a portfolio view of its information system level security risks) and based on such analysis, prioritize remedial actions and resource allocation.

Optimized: The organization should have near real-time visibility into the status of the weaknesses and remediation activities outlined in system-level POA&Ms. This should be done through automated mechanisms that help ensure that the POA&M is accurate, up to date, and readily available. The organization can identify correlate security weaknesses to identify trends and emerging risks across its portfolio of systems in a near real-time manner, prioritize risk response actions based on its overall risk tolerance and appetite, and demonstrate that risk is being reduced over time.

9. To what extent does the organization ensure that ***information about cybersecurity risks is communicated*** in a timely and effective manner to appropriate internal and external stakeholders?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-37 (Rev. 2): Task M-5 • NIST CSF: Section 3.3 • NIST IR 8170	FY2023	**Ad Hoc** The organization has not defined how cybersecurity risk information is communicated in a timely and effective manner to appropriate internal and external stakeholders.	

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST IR 8286 • OMB A-123 • OMB Circular A-11 • OMB M-19-03 • SECURE Technology Act: s. 1326		**Defined** The organization has defined how cybersecurity risks are identified, documented, and communicated in a timely and effective manner to appropriate internal and external stakeholders. This includes the organizations policies, procedures, and processes for using cybersecurity risk registers, or other comparable mechanisms, to share and coordinate cybersecurity risk activities.	• Cyber/privacy/organizational/enterprise risk management policies, procedures, and strategies • Supply chain risk management policies • System-level risk assessment policies and procedures • Enterprise-level risk assessment policies and procedures • Security assessment policies and procedures • ISCM policies, procedures, and strategies
		Consistently Implemented The organization consistently uses a cybersecurity risk register, or other comparable mechanism to ensure that information about risks is communicated in a timely and effective manner to appropriate internal and external stakeholders with a need-to-know. Furthermore, the organization actively shares information with partners to ensure that accurate, current information is being distributed and consumed. Further, processes to share cybersecurity risk information are integrated with the organization's ISCM processes.	• Cyber supply chain risk assessments (see NIST CSF, section 3.3) • Continuous monitoring reports • CSRR(s) • Organization-wide risk registers • organization (i.e., ERM council) and IT meeting minutes • Risk documentation (e.g., SSPs, SARs, POA&Ms, Risk Assessments, IG reports, GAO reports, vulnerability assessments, privacy assessments, security impact assessments, penetration test results, external vulnerability reporting sources (e.g., SANS Internet Storm Center, US-CERT, CISA, etc.) • Incident Response taskers • Updates to organizationally defined risk appetites/tolerances

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable The organization employs robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of cybersecurity risks across the organization. The dashboard presents qualitative and quantitative metrics that provide indicators of cybersecurity risk. Cybersecurity risks are integrated into enterprise level dashboards and reporting frameworks. The organization ensures that data supporting the cybersecurity risk register, or other comparable mechanism, are obtained accurately, consistently, and in a reproducible format and is used to: • Quantify and aggregate security risks • Normalize information across organizational units • Prioritize operational risk response activities	• CSRR(s) • Organization-wide risk register(s) • Organizational ISCM dashboards • ISCM strategies • Continuous monitoring reports/dashboards • ERM meeting minutes. • Evidence of remedial action taken based on the meeting minutes (e.g., documentation supporting the closure of IG audit recommendations, scan results demonstrating the patching of critical vulnerabilities, evidence of staff assignments to tasks designed to mitigate the most critical risks, plans designed to address lower risks in priority order etc.) • Periodic reviews of risk tolerance levels

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Optimized Using risk profiles and dynamic reporting mechanisms, cybersecurity risk information is incorporated into the organization's enterprise risk management program and used to provide a fully integrated, prioritized, enterprise-wide near real-time view of organizational risks to drive strategic and business decisions. Cyber risks are normalized and translated at the organizational level to support a fully integrated, prioritized, enterprise-wide view of organizational risks to drive strategic and business decisions.	• Current and Target-state cyber risk profile (see NIST CSF, section 3.3) • Organization-wide risk assessments/risk registers • CSRR(s), • Organization-wide risk dashboards • Cyber risk dashboards • Enterprise risk management program artifacts, • New investment documentation • Updates to strategic plans • Evidence of streamlined communication/improved workflow between departments (e.g., new dashboards/risk collaboration solutions)

Assessor Best Practices

Defined: Assessors should collect and review organizational/enterprise risk management policies, procedures, and strategies. These policies, procedures, and strategies should include the processes for utilizing cybersecurity risk registers, or other comparable mechanisms, to share and coordinate cybersecurity risk activities (please refer to metric # 5 of the eval guide for more information on the handling of cybersecurity risk registers). These documents should also describe how these processes are integrated into the organization's ERM and ISCM processes and clearly identify all appropriate internal and external stakeholders, as well as specify how cybersecurity risk is documented and disseminated.

Consistently implemented: Assessors should obtain evidence that the cyber risk register(s) are maintained in accordance with NIST IR 8286 and communicated with the appropriate organizational and mission owners, as well as those involved in the ERM and ISCM processes. These risk register(s) provide a formal vehicle for contextualizing, sharing, and coordinating cybersecurity risk activities with organizational management. Therefore, IG assessors should reconcile the information recorded in the cyber security risk register to source documentation (e.g., continuous monitoring reports, system security plans, privacy assessments, security assessment reports, supply chain risk assessments, penetration test results, vulnerability assessments, IG reports, etc.) to confirm that the information included in the cyber risk registers is complete, accurate, and current.

Managed and measurable: Assessors should observe the organizational dashboards that management has implemented and uses to monitor its portfolio of cybersecurity risks. These dashboards should provide the organization with the ability to monitor the qualitative and quantitative metrics documented in the organizational policies, procedures, and/or strategies. These dashboards should provide visibility into events that may be indicators of cybersecurity risk, and tie to cyber risk registers. Assessors should also ensure that the cyber risk register quantifies and

aggregates security risks, normalizes information across organizational units (e.g., bureaus/departments/offices) and tiers (organizational/mission/system), as well as supports a prioritized operational risk response. (Please see NIST IR 8286 series for more information on the development and uses of cyber risk registers, specifically Chapters 3.8, 3.9, and 4 for guidance on how to leverage cyber risk registers as an input to the broader Enterprise Risk Register). Moreover, IG assessors should collect artifacts to ensure that operational risk responses are defined (and occur) in accordance with the scoring presented by the cyber risk register.

Optimized: The organization utilizes the results of the risk assessments conducted at all three tiers of the risk management hierarchy to develop one or more Cybersecurity Framework Profile which express the organization's current and target-state. The profile(s), and other organizational reporting mechanisms (e.g., CSRRs, ERM dashboards, etc.) align cybersecurity outcomes with mission/business requirements, organizational risk appetite, and defined risk tolerances to provide a nearly real-time view of organizational risk. Assessors should also confirm that these artifacts are being used to drive strategic and business decisions.

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?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-39 • NIST 800-207, Tenets 5 and 7 • NIST IR 8286 • OMB A-123 • OMB M-22-09, Federal Zero Trust Strategy, Security Orchestration, Automation, and Response • CISA Zero Trust Maturity Model, Pillars 2-4	Core	**Ad Hoc** 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.	
		Defined 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.	• Organizational risk management policies, procedures, and strategies; • These automated solutions may include a Governance Risk and Compliance solution, spreadsheets, dashboards, shared information in automated workflow solutions, but should include cyber risk registers and allow stakeholders to access the risk information based on their need-to-know.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented 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.	• Risk Management documentation (ex. SSP/RAs, SARs, etc.); • Internal communications to stakeholders about risk (ex. emails, meeting minutes, etc.); • Enterprise wide POA&Ms; • System level POA&Ms; • GRC dashboards/reports; • CSRR(s).
		Managed and Measurable 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.	• GRC dashboards/reports; • CSRR(s); • Threat model exercise reports; • Lessons learned; • Continuous monitoring dashboards/reports (e.g., CDM and SIEM outputs/alerts/reports, vulnerability management dashboards, etc.).
		Optimized 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.	• Enterprise risk profiles • Enterprise-wide and component-level risk management dashboards; • Budget/investment/staffing documentation; • Updates to ERM program documentation, polices, procedures, and strategies; • Target-state enterprise architecture documentation updates (e.g., desired state EA and a roadmap to address any gaps with near real-time updates), etc.; • GRC dashboards/reports.

Assessor Best Practices
Defined: Assessors should obtain organizational risk management policies, procedures, and strategies and ensure they define the requirements of 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. **Consistently implemented:** Assessors should observe and collect artifacts from the organization's automated risk management solution(s) to confirm that the organization has implemented the process outlined in its policies and procedures for centrally managing its risk management process. **Managed and measurable:** Assessors should collect evidence that demonstrates the organization's use of automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact to organizational systems and data integrated with the organization's ERM process. **Optimized:** Assessors should collect evidence demonstrating that 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. Organizations may maintain threat risk/loss scenario modeling information in a business impact assessment and the results of this modeling should act as an input to the CSRR. Moreover, organizational automate controls where practicable, and organizational GRC solution(s) leverage OSCAL to facilitate/automate the security control assessments and to document its SSPs and POAMs, where possible.

11. Provide any additional information on the effectiveness (positive or negative) of the organization's ***risk management*** program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
	Annual	**Ad Hoc**	•
		Defined	•
		Consistently Implemented	•
		Managed and Measurable	•

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Optimized	•

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized:

Supply Chain Risk Management (SCRM)			
12. To what extent does the organization ***use an organization wide SCRM*** strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services?			
Criteria	**Review Cycle**	**Maturity Level**	**Suggested Standard Source Evidence**
• NIST SP 800-53 (Rev. 5): PM-30, SR-1, and SR-2 • NIST SP 800-161 (Rev. 1) • NIST IR 8276 • The Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13, Sub chap. III and Chap. 47, P.L. 115-390) • National Counterintelligence Strategy • OMB M-22-18	FY2023	**Ad Hoc** The organization has not defined and communicated an organization wide SCRM strategy.	
		Defined The organization has defined and communicated an organization wide SCRM strategy. The strategy addresses: • SCRM risk appetite and tolerance • SCRM strategies or controls • Processes for consistently evaluating and monitoring supply chain risk. • Approaches for implementing and communicating the SCRM strategy. • Associated roles and responsibilities	• Organizational SCRM policies, procedures and strategies that addresses the SCRM role and responsibilities; • SCRM policies and procedures include the organization's risk profile and persistent threats, and appropriate controls; • SCRM processes and monitoring strategies; baseline for assessing SCRM risks to IT assets, including threats to the IT system and assets and the supply chain

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		<u>Consistently Implemented</u> The organization consistently implements its SCRM strategy across the organization and uses the strategy to guide supply chain analyses, communication with internal and external partners and stakeholders, and in building consensus regarding the appropriate resources for SCRM. Further, the organization uses lessons learned in implementation to review and update its SCRM strategy in an organization defined timeframe.	• SCRM Risk analysis and evaluation documents; • Evidence of SCRM threat analysis/evaluation/scenario; • Evidence of SCRM vulnerability assessment and testing; • Evidence of SCRM internal and external communication with stakeholders; • Log showing lessons learned used to update the SCRM strategy; • Evidence of communication regarding issues and challenges in reducing the risk of a compromise to products in their supply chain; • Security control mapping of SCRM security characteristics to cybersecurity standards and best practices solutions; • Where applicable, evidence of SCRM suppliers and third-party partners routine assessment and audits.
		<u>Managed and Measurable</u> The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its SCRM strategy and makes updates, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	• Evidence of SCRM qualitative and quantitative metrics were collected. • Templates to support SCRM data is obtained accurately, consistently, and in a reproduceable format. • Change logs showing the data was used to make program improvements.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Optimized The organization's SCRM strategy is fully integrated with its enterprise risk management strategy and program. On a near real-time basis, the organization actively adapts its SCRM strategy to respond to evolving and sophisticated threats.	• Evidence to support that the organization has fully integrated (enterprise-wide) risk based SCRM program that can adjust to emerging (evolving) or near real-time threats. • Evidence of trend analysis performed showing that SCRM related threats have reduced over time based on actions taken by the organization.

Assessor Best Practices

Defined:

Consistently Implemented: Review audits and records to ensure the contractor is in conformance with contractual obligations.

Managed and measurable: Review changes to the program to see that metrics were used to determine the effectiveness of the organization SCRM policies and procedures.

Optimized:

13. To what extent does the organization ***use SCRM policies and procedures*** to manage SCRM activities at all organizational tiers?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53 (Rev. 5): SR-1 • NIST SP 800-161 (Rev. 1)	FY2023	**Ad Hoc** The organization has not defined and communicated its SCRM policies, procedures, and processes.	Intentionally Blank

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST CSF: ID.SC-1 and ID.SC-5 • NIST IR 7622 • NIST IR 8276 • NIST IR 8419 • The Federal Acquisition Supply Chain Security Act of 2018 • DHS's ICT Supply Chain Library • Securing the Software Supply Chain	FY2023	**Defined** The organization has defined and communicated its SCRM policies, procedures, and processes. As appropriate, the policies and procedures are guided by the organization wide SCRM strategy (metric #11). At a minimum, the following areas are addressed: • Procedures to facilitate the implementation of the policy and the associated baseline supply chain risk management controls as well as baseline supply chain related controls in other families. • Purpose, scope, SCRM roles and responsibilities, management commitment, and coordination amongst organization entities.	• SCRM policies and procedures outline the roles, and responsibilities, management commitment and coordination amongst stakeholders; • SCRM controls and baselines to other related controls in other control families, including the organizations risk profile and persistent threats.
	FY2023	**Consistently Implemented** The organization consistently implements its policies, procedures, and processes for managing supply chain risks for [organizationally defined] products, systems, and services provided by third parties. Further, the organization uses lessons learned in implementation to review and update its SCRM policies, procedures, and processes in an organization defined timeframe.	• Evidence to support that the organization collects and uses lessons learned in updating or implementing SCRM policies, procedures and processes in a timely manner. • Evidence to determine that the organization used the lessons learned to make program or process improvements to reduce the overall organization's risk.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
Same Previous List	FY2023	**Managed and Measurable** The organization monitors, analyzes, and reports on the qualitative and quantitative performance measures used to gauge the effectiveness of its SCRM policies and procedures and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format. The organization has integrated SCRM processes across its enterprise, including personnel security and physical security programs, hardware, software, and firmware development processes, configuration management tools, techniques, and measures to maintain provenance (as appropriate); shipping and handling procedures; and programs, processes, or procedures associated with the production and distribution of supply chain elements.	• Evidence to determine that the organization monitors, analyzes and reports on the quantitative and qualitative metrics to determine the effectiveness of its SCRM policies and procedures. • Review evidence and artifacts to determine whether SCRM data supporting the metrics is obtained accurately, consistently and in a reproducible format, such as using SCRM Dashboards/platforms (e.g., Archer Integrated Risk Management (IRM))
Same Previous List	FY2023	**Optimized** In a near real-time basis, the organization can update its SCRM policies, procedures, and processes, as appropriate, to respond to evolving and sophisticated threats.	• Evidence to support that the organization has fully integrated (enterprise-wide) risk based SCRM program that can adjust to emerging (evolving) or near real-time threats. • Evidence of trend analysis performed showing that SCRM related threats have reduced over time based on actions taken by the organization.

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
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?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• The Federal Acquisition Supply Chain Security Act of 2018 • NIST SP 800-53, Rev. 5: SA-4, SR-3, SR-5 and SR-6 (as appropriate) • NIST SP 800-152	Core	**Ad Hoc** 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.	Intentionally Blank

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-161 (Rev. 1)NIST 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 • CSF: ID.SC-2 through 4 • CIS Top 18 Security Controls v.8: Control 15 • Cloud computing contract best practices • FedRAMP standard contract clauses; Cloud Computing Contract Best Practices • DHS's ICT Supply Chain Library	Core	**Defined** 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 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 utilize 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.	• SCRM Policies, procedures, and processes • Evidence that the policies, procedures, and processes have been published, communicated, and prioritized throughout the organization, including communication with external shareholders. • Evidence that the organization has communicated its policies, procedures, and processes for ensuring that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and SCRM requirements, to all stakeholders (emails, list, web links, forums, seminars, etc.)

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
Same Previous List	Core	**Consistently Implemented** 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 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.	• Organizationally defined documentation showing suppliers, contractors, or service providers are being sampled to ensure SCRM requirements are being assessed to identify risk. • Organizational audit or test result checklists, reports, or other forms of official record • Reports from upstream suppliers indicating changes in suppliers; • Requests for reports and responses from upstream suppliers on regular basis; • Review third-party or software producer's cyber related self-attestations (e.g., FISMA, OMB policy, and applicable NIST guidance); • Evidence in form of recent audits, internal reports, recent system scans and reviews, along with coordination with other agencies.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
Same Previous List	Core	**Managed and Measurable** 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 maintain situational awareness into the supply chain risks.	• Qualitative and quantitative metric reports of contractor or external providers to demonstrate products, systems, and services provided are effectively and consistently tracked. • Verify that the defined processes for collecting qualitative and quantitative metrics were communicated to all levels of the organization (websites, emails, etc.); • Evidence that the organization used qualitative and quantitative metrics results to support policy, procedure, or program updates. • Review the organization's recent scans, incident reports, and trend analysis. • Evidence of a quality control process and procedures in place to ensure data supporting metrics are obtained accurately, consistently, and in a reproducible format. • Supply chain risk evaluations are incorporated into the organization's continuous monitoring program (ISCM).
Same Previous List	Core	**Optimized** 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.	• SCRM assessment reports from external providers and evidence that reports have led to change within the organization acquisition tools, methods, and processes in near real-time. • Evidence to support that the organization has fully integrated (enterprise-wide) risk based SCRM program that can adjust to emerging (evolving) or near real-time threats. • Evidence of trend analysis performed showing that SCRM related threats have reduced over time based on actions taken by the organization.

Assessor Best Practices
Defined: Policies should indicate how and what products, components, systems, and services will be accepted into the organization under the organization SCRM strategy and should address at least 80% of the required components. **Consistently Implemented:** Audit evidence should indicate that contractors, service providers, or other entities adhere to security and SCRM requirements. Sampling documents should be from all levels of the organization; observe evidence from the selected sample systems; verify that more than 75% of the sampled systems complied with the SCRM requirements. **Managed and measurable:** Should indicate the organization measures external providers to ensure they are meeting the organization's defined policies and procedures. **Optimized:**

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

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53 (Rev. 5): SR-11 (1)(2)	FY2024	**Ad Hoc** The organization has not defined and communicated its component authenticity policies and procedures.	Intentionally Blank

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-161 (Rev. 1) • OMB M-22-18 • NIST SP 800-218	FY2024	**Defined** 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.	• Anti-counterfeiting policies, procedures, and processes support tamper resistance and provide a level of protection against the introduction of malicious code. • Evidence that Anti-counterfeiting policies, procedures, and processes have been published, communicated, and prioritized throughout the organization, including communication with external shareholders. • Policies and procedures defining audits and/or scanning for counterfeit system components. • Evidence that the organization has communicated its policies, procedures, and processes for ensuring that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and Anti-counterfeiting requirements.
	FY2024	**Consistently Implemented** 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.	• Organizationally defined documentation showing employee training to detect counterfeit system components (including hardware, software, and firmware). • Reports for configuration control over organization-defined system components awaiting service or repair and serviced or repaired components awaiting return to service. • Organizational scans for counterfeit system components.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
Same Previous List	FY2024	**Managed and Measurable** 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.	• Audits of scans for counterfeit system components showing historical trends of counterfeit system components. • Qualitative and quantitative metric reports of component authenticity. • Documentation showing component authenticity controls incorporated into the agency's continuous monitoring practices. • Evidence that the organization used qualitative and quantitative metrics results to support policy, procedure, or program updates.
Same Previous List	FY2024	**Optimized** 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.	• Anti-counterfeiting assessment reports from external providers and evidence that reports have led to change within the organization acquisition tools, methods, and processes in near real-time. • Evidence to support that the organization has fully integrated (enterprise-wide) risk based Anti-counterfeiting program that can adjust to emerging (evolving) or near real-time threats. • Evidence of trend analysis performed showing that Anti-counterfeiting related threats have reduced over time based on actions taken by the organization.

Assessor Best Practices
Defined: Verify policy and procedures are in place that include the means to detect and prevent counterfeit components from entering the organization's systems. The policy and procedures should include elements related to configuration control over organizationally defined system components that are awaiting repair and service, or repaired components awaiting return to service and requirements and procedures for reporting counterfeit system. **Consistently Implemented:** Verify that the agency has identified designated personnel or roles that require anti-counterfeit training. Review audit evidence demonstrating designated personnel or roles have completed training to detect counterfeit system components (including hardware, software, and firmware). Verify the agency has defined system components required to be maintained under configuration control. Review scan reports designed to detect counterfeit components and verify they are complete and accurate. **Managed and measurable:** Obtain evidence demonstrating component authenticity controls are incorporated into the agency's continuous monitoring practices. Obtain evidence that the agency uses reproducible qualitative and quantitative measurements that provide results to support anti-counterfeiting policy, procedure, or program updates. **Optimized:** Review anti-counterfeiting assessment reports from external providers. Verify the agency performs trend analyses demonstrating that anti-counterfeiting related threats have reduced over time based on actions taken by the agency. Review recent updates to the agency's supply chain risk management policies and procedures to determine if agency is responding to evolving and sophisticated threats in near real-time.

16. Provide any additional information on the effectiveness (positive or negative) of the organization's ***supply chain risk management*** program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
	Annual	**Ad Hoc**	•
		Defined	•
		Consistently Implemented	•
		Managed and Measurable	•

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Optimized	•

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized:

Configuration Management (CM)

17. To what extent have the ***roles and responsibilities*** of configuration management stakeholders been (1) defined, (2) communicated, and (3) implemented across the agency, and (4) appropriately resourced?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53 (Rev. 5): CM-1 • NIST SP 800-128: Section 2.4 • Green Book: Principles 3, 4, and 5	FY2024	**Ad Hoc** 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.	Blank
		Defined 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.	• Organizational charts • Agency wide information security policies and procedures relating to the implementation of configuration management policies and controls. • Screenshots/observations detailing how configuration management roles and responsibilities are communicated throughout the organization. • Evidence of conducting Cybersecurity Workshops/Discussions.
		Consistently Implemented Individuals are performing the roles and responsibilities that have been clearly defined across the organization via documented policies and procedures.	• Configuration management testing evidence/documentation

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable 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.	• Information technology budget established for agency-wide configuration management protocols and controls. • Examples of stakeholders performance reviews/appraisals. • Cyber Security Framework scorecard used for assessing accountability. • Senior leadership briefings.
		Optimized The organization continuously evaluates and adapts its configuration management-based roles and responsibilities to account for a changing cybersecurity landscape.	• Evidence of tracking configuration management metrics • Continuous monitoring using automatic feeds. • Dashboard monitoring.

Assessor Best Practices

Defined:

Consistently Implemented:

- Interview stakeholders to determine whether adequate resources have been planned for and provided to implement the organizations CM program.

Managed and measurable:

Optimized:

18. To what extent does the organization utilize an ***enterprise wide configuration management plan*** that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53 (Rev. 5): CM-9 • NIST SP 800-128: Section 2.3.2	FY2024	**Ad Hoc** The organization has not developed an organization wide configuration management plan with the necessary components.	
		Defined The organization has developed an organization wide configuration management plan that includes the necessary components.	• Enterprise-Wide Configuration Management Plan. • Change Control Board charter. • Change Control Board procedures. • Policy requiring use of FedRAMP for new cloud service provider solutions.
		Consistently Implemented The organization has established a CCB that is used to consistently implement an organization wide configuration management plan and has integrated its plan with its risk management and continuous monitoring programs. In addition, roles and responsibilities are clearly defined. Further, the organization uses lessons learned in implementation to make improvements to its plan.	• Evidence that appropriate risk assessment activities were performed. • Evidence showing configuration changes for which the organization's change control/change management processes would apply. • Evidence of lessons learned being performed for configuration management activities and plans. • Change Control Board meeting minutes.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable 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.	• Evidence of tracking configuration management metrics • Configuration management testing evidence/documentation (sample testing, etc.). • Establishing a lessons learned function and tracking process (possibly a tracking database). • Establishing and tracking a change workflow. • Evidence of Change Control Board request process and monitoring.
		Optimized 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).	• Participation in a Continuous Diagnostics and Mitigation program. • Implementation and tracking of automated change management processing allowing near real-time change and approvals.

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized:

19. To what extent does the organization utilize ***baseline configurations*** for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53 (Rev. 5): CM-2 and CM-8 • NIST CSF: DE.CM-7 and PR.IP-1 • BOD 23-01 • CIS Top 18 Security Controls: Control 4	FY2023	**Ad Hoc** The organization has not established policies and procedures to ensure that baseline configurations for its information systems are developed, documented, and maintained under configuration control and that system components are inventoried at a level of granularity deemed necessary for tracking and reporting.	

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Defined The organization has developed, documented, and disseminated its baseline configuration and component inventory policies and procedures.	• Enterprise level Configuration Management policy(ies) for developing, testing, approving, and managing baseline configurations. • Enterprise level Configuration Management procedures for developing, testing, approving, and managing baselines. • System level Configuration Management policy(ies) for developing, testing, approving, and using baseline configurations (if applicable). • System level Configuration Management procedures for developing, testing, approving, and managing baselines (if applicable); • Asset Inventory policy and procedures; • Emails, web postings, or other means of communicating Baseline Configurations policies and procedures to stakeholders at all levels of the organization.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented The organization consistently records, implements, and maintains under configuration control, baseline configurations of its information systems and an inventory of related components in accordance with the organization's policies and procedures. Further, the organization uses lessons learned in implementation to make improvements to its baseline configuration policies and procedures.	• Baseline settings documentation (build documentation, forms, spreadsheet, exports from tools, etc.) for end user devices (workstations, I/O devices, etc.), and network devices (routers, switches, etc.). • Baseline settings documentation for select sample systems (e.g., servers) and hardware and software components. • Baseline settings documentation for select sample user and service applications (e.g., MS Office, web, SQL, etc.). • For select sample systems, obtain evidence the organization has updated the baseline configuration IAW organizationally defined timelines. • Sample configuration control artifacts showing changes to baselines were processed IAW organizationally defined configuration control board (CCB) procedures. • Reports (preferably in machine readable format such as CSV) from scanning tools used to monitor configurations. Reports for all asset types and for multiple timeframes (for trend analysis). • Sample deviation detection response actions (baseline redeployment logs, service tickets, etc.) • Sample after actions reviews indicating lessons learned. • System Security Plans and other risk documentation • Policy or process updates in response to lessons learned.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable The organization employs automated mechanisms (such as application whitelisting and network management tools) to detect unauthorized hardware, software, and firmware and unauthorized changes to hardware, software, and firmware.	• Evidence of a use of Asset Baseline monitoring tool(s) • Host-based Intrusion Prevention System (HIPS) policies • Continuous Diagnostics and Mitigation (CDM) dashboards • Observation and data analysis of information in network management tools • Automated mechanisms to detect presence of unauthorized hardware, software, and firmware components (including remote and mobile)
		Optimized The organization uses technology to implement a centralized baseline configuration and information system component inventory process that includes information from all organization systems (hardware and software) and is updated in a near real-time basis.	• Evidence of a Configuration Management Database (CMDB) or related tool that includes baselines with historical retention for roll back. • Screenshots of rules configured in tools to perform automatic actions in correlation with other tools. • Reports from tools showing the integration and real-time actions performed.

Assessor Best Practices
Note:** Assessment of "inventory" actions is duplicate criteria from metrics 1-3. Assessors should not assess inventory to determine maturity of ***this metric. Focus ONLY on baselines. Future iteration of the Metrics will correct and clarify this. **Defined**: Assessors should assess organizational policies and procedures to ensure a formal process exists to develop, test, and approve baselines in a controlled and systematic manner. Ensure the policies and procedures align with current NIST guidance and DHS requirements (e.g., BOD 23-01). Ordinarily, policies and procedures will use organizationally accepted predefined standard (NIST, STIG, NSA, CIS guide, etc.) as a starting point for the *tailored* technical configurations included in the configuration baselines, however there may be times when predefined standards don't exist. In such instances, assessors should verify processes to work with vendors to develop, test, and document customized baseline standards. Policies and procedures should also include a process by which organizations manage and approve deviations to configurations baselines (i.e., how the rational for deviating from the hardening guides are justified and documented). Policies and procedures

should also define how the organization controls updates and maintenance of the baselines via a CCB. Policies and procedures should define how the organization will monitor adherence (e.g., scanning and analysis) and respond to deviations (e.g., redeployment logs, service tickets, incident reports, etc.) after deployment. In addition, assessors should consider the results of metrics 1-3 when testing this metric and confirm that the organization has a defined process for ensuring that its system inventory is complete and authorization boundaries are well documented. Finally, policies and procedures should establish a process by which management leverages its configuration management baselines as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture, as well as ensuring that the baselines are reflective of the organization's EA. Asset inventory information should be included or referenced in the Configuration Management Plan.

Consistently Implemented: Assessors should request baseline documentation for all information system, hardware, and software asset types to ensure baselines have been created for all assets in the inventories assessed in Risk Management metrics 1-3. If the assessor finds, through sample testing in this metric that the systems, hardware, or software inventory is incomplete, this should be considered in the maturity determination. Examples include end user devices (workstations, I/O devices, etc.), mobile devices, and information systems (servers and associated hardware and software components). Evidence can be forms, build documents, spreadsheets, tool exports, or other means showing the configuration items (e.g., software/applications/databases, hardware/firmware, locations/offices, hardware, etc.) and technical configuration settings (e.g., NVD implementations). Evidence should show that the organization-tailored baselines disable device services or features that are not necessary to support mission functions and/or are considered inherently risky (and do not have compensating controls). Also, the assessor should ensure that software installed on sampled devices is limited to authorized individuals to ensure the principle of least privilege and least access. For each baseline type assessors should look for a formal approval to deploy.

Assessors should assess the organization's implementation of baselines to verify the application of uniform configurations to all information system, hardware, and software asset types, as well as at multiple levels (enterprise, program offices, subordinate units, etc.). Assessors should obtain baseline configuration scans for a sample of systems (sample size is at the discretion of the OIG) to verify baselines have been applied IAW defined policies and processes. For centrally managed environments, evidence should show how the approved baseline is deployed to all organizational end user devices, network devices (switches, routers, firewalls, etc.) and servers. Evidence should also demonstrate that servers are centrally managed (SCCM, Puppet, manual images, etc.), where practical. If not centrally managed, assessors should sample an organizationally determined number of baseline processes to determine if established baselines are being deployed IAW defined policy(ies). In hybrid environments where some services are performed at the enterprise level and in program offices, sample systems should be taken from all relevant areas to evaluate implementation.

Assessors must also determine if the organization is managing and monitoring the deployed baselines. A common method for assessing compliance with approved technical configurations is to evaluate common configuration enumeration (CCE) scans (using tools such as Nessus) to determine if there are systems that deviate from their approved baseline. CCE scans are not the only method, but one that is commonly available to government agencies. This requires a scanning system configured with all approved baselines as the benchmark for assessing the various systems in the inventory. Assessors should confirm that the baseline configuration scans are run IAW organizationally defined policy and over multiple periods (e.g., months, quarters, etc.) to ensure the effectiveness of monitoring processes. Compare multiple scans to cross reference findings and determine if there is a significant number of repeat findings -this would indicate no action taken. If there are relatively few repeat findings, then that indicates the organization is likely monitoring scans and responding to detected deviations. Assessors should also review

actions taken when deviations are detected. For example, assessors can review redeployment logs and subsequent scan results to see if the issues were resolved, collect evidence of compensating controls if a configuration change cannot be remediated without a serious impact to the mission, or review service desk tickets for manual resolution and subsequent scan results to see if issues were resolved.

When evaluating baseline configuration monitoring using CCE scans, assessors should assess the accuracy of the information systems, hardware, and software asset inventories assessed in Risk Management metrics 1-3 to ensure consistency in metric reporting. Assessors may do this by confirming that the system authorization boundaries defined in the agency risk documentation include references to all of the sw/hw identified in the CCE scans. Additionally, assessors should assess compliance with BOD 23-01 (are all IP's being scanned, is the discovery frequency adhered to, etc.…) as part of this process.

Finally, assessors should determine if the organization has performed lessons learned exercises on its CM policies or procedures. AAR notes from CCB sessions, or emails from those implementing the processes are potential examples as well.

Managed and Measurable: Assessors should verify that the organization employs automation to perform the creation, management, monitoring and response tasks discussed at the Consistently Implemented level metric. System inventory tools, Configuration Management Database (CMDB) or related tools, and Asset Baseline Monitoring (ABM) tools are some solutions that may be leveraged to automate the configuration management process. Assessors should also determine if application whitelisting is being used by the organization to limit its attack surface.

Optimized: Assessors observe evidence of centralized tie-in and near real-time use of management process, such as integration of system inventory, CMDB or related tools, and ABM tools. For example, if a system is detected with a new hardware component, a real-time process kicks off to query system inventory tool to determine if it's been added to the inventory, and then a query to the CMDB to determine if they change was approved. Same theory applies to software changes (e.g., adding/removing software, changing software configuration, etc.) and other baseline configuration deviations discussed in earlier maturity levels.

20. To what extent does the organization utilize ***configuration settings/common secure configurations*** for its information systems?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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 • EO 14028: Sections 4, 6, and 7 • OMB M-22-09 • OMB M-24-04	Core	**Ad Hoc** The organization has not established policies and procedures for ensuring that configuration settings/common secure configurations are defined, implemented, and monitored.	
		Defined 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 secure configurations (hardening guides) that are tailored to its environment. Further, the organization has established a deviation process.	• Policies and procedures for system hardening/configuration setting management, including processes for managing deviations; • Organization's tailored hardening guides

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• BOD 23-01 • CIS Top 18 Security Controls: Controls 4 and 7 • CISA Cybersecurity Incident Response Playbooks		**Consistently Implemented** The organization consistently implements, assesses, and maintains secure configuration settings for its information systems based on the principle of least functionality. Further, the organization consistently uses SCAP-validated software assessing (scanning) capabilities against all systems on the network (in accordance with BOD 23-01see) 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	• Evidence of vulnerability scanning conducted for the last four quarters • Acceptable deviation/exception lists/justifications for organizationally tailored hardening guides; • Observation and analysis of Security Content Automation Protocol (SCAP) tools to determine coverage and use of rulesets and frequencies; • Lessons learned incorporated into the secure configuration policies and procedures.
		Managed and Measurable 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 makes appropriate modifications in accordance with organization-defined timelines.	• Dashboards that highlight in real-time the devices on the network and their compliance with the agency's baselines
		Optimized The organization deploys system configuration management tools that automatically enforce and redeploy configuration settings to systems at frequent intervals as defined by the organization, or on an event driven basis.	• Evidence of frequent, enforced system configurations; • Evidence of event-triggered configuration, Automated configuration from Continuous Diagnostics and Mitigation (CDM) events' • Automated routing/approval process and queues to enforce process and prevent out-of-sequence events

Assessor Best Practices
Defined: Assessors should verify that the organization maintains security configuration standards for all asset types, including: • End user devices (workstations, laptops, etc.) • Input and output devices (multifunction devices, printers, scanners, copiers, etc.) • Operating systems and software (CIS Control 5.1) • Network devices (CIS Control 11.1) • Servers and applications, including web applications Assessors should verify that the organization has developed secure images or templates for all systems in the enterprise based on the organization's approved configuration standards (CIS Control 5.1 and 5.2). Assessors should verify that the organization has documented standards for defining (and justifying) acceptable deviations from externally established hardening guides (e.g., STIGs) as well as deviations from internally developed (customized) hardening guides. **Consistently Implemented:** For a sample of systems, assessors should conduct vulnerability scanning (including at the operating system, network, database, and application levels) to assess the implementation of the agency's configuration settings/baselines. Assessors may observe the tools used by the organization to conduct vulnerability scanning and verify the use of credentialed scans and coverage of devices/applications. Assessors should also analyze tool settings to verify coverage of scanning, rulesets, and schedules. Assessors should validate that application-level scanning is conducted for all public facing websites. Further, the organization should demonstrate that it proactively scans all systems on its network (at an organization defined frequency; preferably weekly) for vulnerabilities and addresses discovered weaknesses (CIS Control 3). The scanning should cover public-facing web applications (see CIGIE Web Application report for additional details). The organization should be using a dedicated account for authenticated scans which should not be used for other administrative activities and should be tied to specific machines at specific IPs (CIS Control 3.3). Furthermore, assessors should verify that the organization is using up-to-date SCAP compliant scanning tools [e.g., Nessus, BigFix, SCAP Compliance Checker, etc.]. In addition, at Consistently Implemented, assessors should verify that vulnerabilities identified through scanning activities, including for public facing web applications, are consistently remediated for sampled systems. Finally, the assessor should ensure that all assets discovered during the BOD 23-01 scans are configured IAW organizational policy and best practices and the organization scans for known code-based and configuration-based vulnerabilities. **Managed and Measurable:** The organization should use automation, such as system configuration management tools to monitor security configuration compliance for the devices connected to its network and measure/report on the effectiveness of its configuration management processes accordingly. The difference between level 4 and level 5 is that at level 5, the organization is using automation, in near real-time, to redeploy configuration settings as deviations are identified. The intent at level 4 is to verify that the agency has readily available visibility into the security configurations for the devices connected to its network. At level 4, the organization should demonstrate that it utilizes system configuration management tools to measure the settings of operating systems and applications to look for deviations from standard image configurations.

Optimized: The organization should deploy automation to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur (CIS Control 5.5). At level 5, the organization should demonstrate that it uses system configuration management tools to automatically redeploy settings.

21. To what extent does the organization utilize ***flaw remediation processes,*** including ***patch management***, to manage software vulnerabilities?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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 • EO 14028: Sections 3 and 4 • OMB M-22-09	Core	**Ad Hoc** The organization has not developed, documented, and disseminated its policies and procedures for flaw remediation, including for mobile devices (GFE and non- GFE).	
		Defined 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.	• Patch management/flaw remediation policies and procedures; • Configuration management policies and procedures; • BYOD policies and procedures.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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		**Consistently Implemented** 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.	• Nmap/LanSweeper scans showing all network accessible IP assets; • Screenshots of vulnerability scanning system showing configurations; • Demonstrations of vulnerability scanning tools and processes; • Documentation that shows identification, prioritization, and testing of a patch, hotfix, service pack, and/or AV/Malware update; • Vulnerability scans prior and post update (to prove timeliness); • Patch management reports • Documentation showing lessons learned that were obtained from all levels of the organization and were used to update/enhance policies and procedures. Could be a statement in the policies and procedures change log.
		Managed and Measurable The organization centrally manages its flaw remediation process and utilizes 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.	• Evidence of automated flaw remediation using trusted, verified repositories for operating systems; • Metrics to measure (turnaround) performance and make continuous improvements are reported to appropriate stakeholders; • Evidence of prioritization of testing and patch management based on risk assessment

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Optimized The organization utilizes 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.	• Evidence of automated patch management and software updates using trusted, verified repositories for all applications and network devices; • Integration with ISCM and IR programs to account for and utilize all flaw discovery sources

Assessor Best Practices

Defined: Assessors should evaluate the organization's defined policies and procedures for flaw scanning, analysis, and remediation to ensure they address **all network addressable IP-assets** (which should match inventories assessed in the risk management domain metrics 1-3). The policies and procedures should also define how the network addressable IP assets are documented (e.g., spreadsheet, form, database, etc.), grouped (e.g., function, location, etc.), prioritized (e.g., high, moderate, low risk assets), and updated (e.g., scanning frequency). The scope of these policies and procedures should include, but not be limited to, applications (COTS and GOTS), servers, workstations, input and output devices, network devices, and mobile devices (GFE and non-GFE in an approved BYOD environment). The policies and procedures should, at minimum define the following processes: asset discovery, vulnerability scanning, results analysis, patch testing, and patch management.

Consistently implemented: Assessors should determine if the organization implements its defined flaw scanning, analysis, and remediation policies, procedures, and processes for **all network addressable IP-assets**. BOD 23-01 focuses on scanning, which is the basis for flaw remediation. An organization cannot effectively remediate flaws if it is not properly analyzing the scans and prioritizing the results. Assessors assess if agencies are reviewing scans to identify patch lag, false positives, associate with high value assets, etc. Areas to assess to ensure consistency with BOD's 22-01 and 23-01, include validating organizations:

- perform asset discovery every 7 days (BOD 23-01)
- conduct credentialed vulnerability scanning every 14 days (BOD 23-01)
- ensure vulnerability detection signatures are updated at an interval no greater than 24 hours
- prioritize known exploited vulnerabilities (KEV), according to the CISA-managed catalog, and remediates 2021 and older KEVs within 6 months (BOD 22-01) and all others within two weeks
- ensure that patches, hotfixes, service packs rated as critical vulnerabilities are installed within 15 days (BOD 19-02) or have senior agency approved remediation plans for open findings
- ensure that patches, hotfixes, and service packs rated as a high vulnerabilities are installed within 30 days (BOD 19-02), or have senior agency approved remediation plans for open findings

- implement malicious code protection (e.g. Anti-virus) mechanisms on all computing assets (to the greatest extent possible) to detect and eradicate malicious code, automatically update malicious code protection mechanisms as new releases are available, perform periodic scans of the system, perform real-time scans of files from external sources, and block malicious code execution (NIST SP 800-53 Rev. 5, SI-3)

Assessors, throughout this process, should also confirm that the versions of the EO-critical software leveraged by the organization are currently supported.

Managed and Measurable: One of the major advancements in Managed and Measurable is the focus on automation for operating systems patching (automation for all other assets is at the Optimized level). The organization compares the results of multiple vulnerability scans to detect and correct trends of failing to patch in accordance with required timelines. For Managed and Measurable assessors should be ensuring that the organization are detecting problems with its scan and patch processes (800-53r5 control RA-5(6)). Assessors should validate the accuracy, completeness (e.g., all network addressable IP-assets are considered in the organizational analyses), and reproducibility of the patch reporting and trend analysis performed by the organization.

Optimized: The organization centrally manages its implemented flaw remediation processes and uses automated patch management and software update tools for all network addressable IP-assets. Ensures interoperability among tools used for vulnerability management and configuration management tasks.

22. To what extent has the organization adopted the ***Trusted Internet Connection (TIC)*** program to assist in protecting its network?			
Criteria	**Review Cycle**	**Maturity Level**	**Suggested Standard Source Evidence**
• NIST SP 800-207 • OMB M-19-26 • DHS-CISA TIC 3.0 Core Guidance Documents • NCPS Cloud Interface Reference Architecture	FY2023	**Ad Hoc** The organization has not prepared and planned to meet the goals of the TIC initiative, consistent with OMB M-19-26. Specifically, the agency has not defined and customized, as appropriate, its policies, procedures, and processes to implement TIC 3.0, including updating its network and system boundary policies, in accordance with OMB M-19-26. This includes, as appropriate, the TIC security capabilities catalog, TIC use cases, and TIC overlays. The agency has not defined processes to develop and maintain an accurate inventory of its network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection.	

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Defined The organization has prepared and planned to meet the goals of the TIC initiative, consistent with OMB M-19-26. Specifically, the agency has defined and customized, as appropriate, its policies, procedures, and processes to implement TIC 3.0, including updating its network and system boundary policies, in accordance with OMB M-19-26. This includes, as appropriate, incorporation of TIC security capabilities catalog, TIC use cases, and TIC overlays. The agency has defined processes to develop and maintain an accurate inventory of its network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection.	• Organization's TIC implementation plan; • Organization's TIC strategy; • Organization's TIC policy; • Organization's boundary policy(ies); • Organization's network policy(ies) • Contract/SOW/Task Order with MTIPS provider
		Consistently Implemented The organization consistently implements TIC requirements based on OMB M-19-26. This includes consistent implementation of defined TIC security controls, as appropriate, and ensuring that that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. The agency develops and maintains an accurate inventory of agency network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection.	• Network Diagrams showing external connections; • Inventory of external connections (see Additional Information); • Organization’s TIC reference architecture; • Einstein alerts; • Architecture Design and Diagrams – Data flow, transport, key security, monitoring services and capabilities, and policy enforcement points (PEPs)

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable The organization, in accordance with OMB M-19-26, DHS guidance, and its cloud strategy is ensuring that its TIC implementation remains flexible and that its policies, procedures, and information security program are adapting to meet the security capabilities outlined in the TIC initiative, consistent with OMB M-19-26. The organization monitors and reviews the implemented TIC 3.0 use cases to determine effectiveness and incorporates new/different use cases, as appropriate.	• Review records of current TIC implementation showing changes; • Change records due to any security incident response actions; • Lessons learned reports; • Performance metrics reports; • Risk based decisions for deviation from standard use cases
		Optimized The organization integrates its implementation of TIC 3.0 with the organization's zero trust architecture strategy. Further, for cloud-based environments, the organization provides telemetry on its cloud-based traffic to CISA via the National Cybersecurity Protection System.	• Zero trust architecture (ZTA) strategy; • Telemetry sharing configuration settings screenshots or other forms of evidence; • Telemetry reports showing cloud-based traffic information going to the CISA National Cybersecurity Protection System (NCPS); • Dashboard examples showing integration of ZTA and telemetry.

Assessor Best Practices
***Note:** OMB M 19-26 was published 12 Sep 2019 and agencies had one year (12 Sep 2020) to accomplish the required actions. So, the "planning" cycle that's described in the metric is out-of-date and will be updated in the next version of the metric. Assessors should evaluate based upon current requirements. Policies, procedures, and other required documentation should be defined by this point. **Defined:** Assessors should ensure its policies and procedures require that the organization maintain an inventory of external connections which contains all of the required elements for each connection (service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data.) TIC Processes should define how the agency will maintain the inventory information. Maintenance of the inventory

information includes defining how often the inventory information is updated and how changes to the inventory are approved. The policies and procedures should also define how the organization leverages TIC use cases, Security Capabilities Catalog, and TIC overlays – please see CISA TIC 3.0 Overlay Handbook, section 5 for more information on these categories) when selecting a vendor service.

Consistently Implemented: Assessors should assess the implementation of TIC use cases and architecture to determine and describe how the agency's implementation meets the 5 TIC 3.0 Security Objectives (TIC 3.0 Program Guidebook, pages 6-8) for *each network connection*. If the agency has many network connections an appropriate sample section should be considered (varying samples each fiscal year to eventually cover all connections is recommended). Assessors should determine if each network connection has implemented a TIC use case and overlay that creates a trust zone tailored to the organization's risk tolerance for that connection.

Managed and Measurable: Assessors should take into consideration any documentation that indicates the agency is monitoring the performance of the TIC use cases and make adjustments as needed. Many factors can cause the organization to modify its use case and make adjustments. Indicators should show a continuous monitoring and proactive approach to remaining flexible.

Optimized: Assessors should review the ZTA strategy and use of TIC use cases for integration. Review logs, alerts, and other telemetry data to determine if the agency is sharing the appropriate telemetry data (section 8 of each Use Case except Cloud, which is section 4.5) with DHS CISA as required. Sharing can be accomplished via the National Cybersecurity Protection system (NCPS) or other approved solution.

23. To what extent has the organization defined and implemented configuration change control activities including:
    - determination of the types of changes that are configuration controlled
    - review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system
    - documentation of configuration change decisions
    - implementation of approved configuration changes
    - retaining records of implemented changes
    - auditing and review of configuration changes
    - and coordination and oversight of changes by the CCB, as appropriate?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53 (Rev. 5): CM-2, CM-3, and CM-4 • NIST CSF: PR.IP-3	FY2024	**Ad Hoc** 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.	
		Defined 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.	• Agency wide change control policies and procedures. • System level change control policies and procedures.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented The organization consistently implements its change control policies, procedures, and processes, including explicit consideration of security impacts prior to change implementation. The organization has clearly defined who is responsible for implementing these changes and validates that they have been implemented correctly. The organization uses lessons learned in implementation to make improvements to its change control policies and procedures.	• Evidence detailing change control request/ticket processing in accordance with policies and procedures. • Evidence of lessons learned being performed for configuration management change control activities and plans. • Evidence detailing how the organization tests security impacts prior to change. • Documented hardware and software changes submitted to an Enterprise Architecture Review Board for review and approval.
		Managed and Measurable 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, ensuring (when necessary) that the organization's CCB is involved in the process. In addition, the organization implements [organizationally defined security responses] if baseline configurations are changed in an unauthorized manner.	• Evidence of monitoring, analyzing, and reporting on configuration management metrics (linked back to the configuration management plan and change control policies).

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Optimized 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 control activities to support risk-based decision making across the organization.	• Screenshots of automated tool or observations of other automated methods capturing data on change control activities. • Automated alerting functionality/notifications relating to capturing the accuracy, consistency, and availability of configuration change control and configuration baseline information. • Integrated dashboard monitoring and analytics. • Integration of the Cyber Security Risk scorecard for use of qualitative and quantitative decision making.

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized:

24. To what extent does the organization utilize a ***vulnerability disclosure policy (VDP)*** as part of its vulnerability management program for internet-accessible federal systems?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53 (Rev. 5): RA-5(11) • OMB M-20-32 • DHS BOD 20-01	FY2023	**Ad Hoc** The organization has not developed, documented, and disseminated a comprehensive VDP.	
		Defined The organization has developed, documented, and publicly disseminated a comprehensive VDP. The following elements are addressed: • The systems in scope • Types of testing allowed • Reporting mechanisms • Timely feedback • Remediation In addition, the organization has updated its vulnerability disclosure handling procedures to support the implementation of its VDP.	• Organization's VDP implementation plan; • Organization's VDP strategy; • Organization's VDP policy; • Organization's vulnerability disclosure handling procedures; • Organization's public notice (e.g., web page posting); • DNS records showing VDP Points of Contact.
		Consistently Implemented The organization consistently implements its VDP. In addition, the organization: • Has updated the relevant fields at the .gov registrar to ensure appropriate reporting by the public. • Ensures that newly launched internet accessible systems and services, and at least 50% of internet-accessible systems, are included in the scope of its VDP. • Increases the scope of systems covered by its VDP, in accordance with DHS BOD 20-01.	• Records of the .gov registrar; • Records showing a newly implemented system was added to the VDP; • Records of a new production system being added to the VDP.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable The organization monitors, analyzes, and reports on the qualitative and quantitative performance measures used to gauge the effectiveness of its vulnerability disclosure policy and disclosure handing procedures. In addition, all internet-accessible systems are included in the scope of the organization's VDP.	• Records showing the measurement of performance measures; • Records of changes to the VDP in response to performance measurements; • Configuration change records showing changes in response to a publicly disclosed vulnerability.
		Optimized On a near real-time basis, the organization actively adapts its vulnerability disclosure policies and procedures and provides information to stakeholders and partners. Within the context of its enterprise risk management program, the organization considers the use of a Bug Bounty program. As appropriate, Bug Bounty programs are implemented in accordance with OMB M-20-32.	• Change records of VDP policies and procedures; • Communication records of dissemination of updated VDP policies and procedures; • Enterprise risk management meeting minutes.

Assessor Best Practices
Defined: Assessors should evaluate the organization's policies and procedures to assess if guidance is consistent with the references described in the maturity level description. Review the organization's public web page and DNS records for the appropriate public VDP posting. Organizational policies should also require the organizational to update the .gov register in a timely manner and describe how the VDP (and underlying inventory) is to be maintained. Review evidence that all levels of the organization have received the VDP policies and procedures for implementation. **Consistently Implemented:** The requirement deadlines are past the initial implementation (2 year after publishing of the BOD). All systems should now be included in the VDP and should now be a requirement for consistently implemented. Evaluating to ensure that newly launched internet accessible systems and services are included in the scope of its VDP will require new systems to be put into production and not all evaluation years may have new systems introduced. The assessor may consider reconciling the systems inventory (and change control tickets associated with newly released internet accessible systems) against those systems outlined in the VDP as a starting point for this assessment. **Managed and Measurable:** Assessors should review performance measurements the organization has implemented to monitor and improve the program. Assessors should also identify any indicators of change to the program based on measurements, recent updates to the VDP, and lessons learned. Assessors should also identify any changes to web applications and web pages in response to publicly reported vulnerabilities (and the timeliness of those changes), which indicates the effectiveness of the VDP. **Optimized:** Assessors should review the VDP policies and procedures change records to evaluate how often the documents were updated and determine what triggered the update. Assessors should consider opportunities to rapidly (in near real-time) update the documents (e.g., updated technology, threat landscape change, etc.). And of those opportunities exist, determine if the organization has taken advantage of them to perform updates timely. Assessors should also review ERM meeting minutes to determine if a risk-based decision was used to decide upon a bug bounty program.

25. Provide any additional information on the effectiveness (positive or negative) of the organization's **configuration management** program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
	Annual	**Ad Hoc**	•
		Defined	•

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented	•
		Managed and Measurable	•
		Optimized	•

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized:

Identity, Credential, and Access Management (ICAM)

26. To what extent have the ***roles and responsibilities*** of identity, credential, and access management (ICAM) stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53 (Rev. 5): AC-1, IA-1, IA-2, PL-4, and PS-1 • NIST SP 800-63-3 • NIST SP 800-63A, B, and C • OMB M-04-04 • OMB M-19-17 • Federal Identity, Credential, and Access Management (FICAM) playbooks and guidance • HSPD 12	FY2023	**Ad Hoc** Roles and responsibilities at the organizational and information system levels for stakeholders involved in ICAM have not been fully defined and communicated across the organization.	
		Defined Roles and responsibilities at the organizational and information system levels for stakeholders involved in ICAM have been fully defined and communicated across the organization. This includes, as appropriate, developing an ICAM governance structure to align and consolidate the agency's ICAM investments, monitor programs, and ensuring awareness and understanding.	• Agency-wide information security policy, ICAM strategy, policies, and procedures; • Business case for agency wide ICAM investments; • Organizational Charts (Organization-wide and at the system level) supporting a defined level of maturity; • Roles and responsibilities including those for developing and maintaining metrics on the effectiveness of identity and access management activities have been defined in policy document(s) and documentation that they have been communicated across the organization; • Documentation that staff are assigned responsibilities for developing, managing, and monitoring metrics on the effectiveness of ICAM activities.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented Individuals are performing the roles and responsibilities that have been defined across the organization. The organization ensures that there is consistent coordination amongst organization leaders and mission owners to implement, manage, and maintain the organization's ICAM policy, strategy, process, and technology solution roadmap.	• Organizational charts (Organization-wide and at the system level) supporting a consistently implemented level of maturity. • OMB ICAM Federal Level Working Groups Meetings & distributed guidance; • Supporting artifacts could include Job descriptions. Evidence of periodic account review. Meeting Records; • Documents or other artifacts may support that individuals are performing in their defined roles.
		Managed and Measurable Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement identity, credential, and access management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	• Supporting documentation that adequate resources have been dedicated to this program; • interview relevant stakeholders and evaluate budget requests; • Supporting evidence of stakeholder accountability will vary. One example could be Working Group Meeting Minutes that record an instance of stakeholders reporting on their responsibilities.
		Optimized In accordance with OMB M-19-17, the agency has implemented an integrated agency-wide ICAM office, team, or other governance structure in support of its ERM capability to effectively govern and enforce ICAM efforts.	• Support that and ICAM governance structure has been implemented which might include: • Organizational charts • A charter or other policy document outlining the objectives and authorities of the governance structure.

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable: To determine whether adequate resources have been dedicated to this program, interview relevant stakeholders and evaluate budget requests.
Optimized:

27. To what extent does the organization use a comprehensive ICAM policy, strategy, process, and technology ***solution roadmap*** to guide its ICAM processes and activities?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53 (Rev. 5): AC-1 and IA-1 • NIST SP 800-207 • NIST CSF: PR.AC-4 and PR.AC-5 • OMB M-19-17 • OMB M-22-09 • DHS ED 19-01	FY2023	**Ad Hoc** The organization has not developed a comprehensive ICAM policy, strategy, process, and technology solution road map to guide its ICAM processes and activities. In addition, the organization has not performed a review of current practices, identified gaps, and developed a transition plan to serve as an input to the ICAM policy, strategy, and technology solution road map.	

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• FICAM • CIS Top 18 Security Controls: Controls 5 and 6		**Defined** The organization has developed a comprehensive ICAM policy, strategy, process, and technology solution road map to guide its ICAM processes and activities. The organization has developed milestones for how it plans to align with Federal initiatives, including strong authentication, the Federal ICAM architecture and OMB M-19-17, and phase 2 of DHS's Continuous Diagnostics and Mitigation (CDM) program, as appropriate.	• ICAM strategy and plans. • ICAM policy and procedures. • ICAM architecture. • Project plan, including milestones, for implementation of strong authentication and single sign-on, as appropriate. • MOA (or similar document) with DHS for CDM program.
		Consistently Implemented The organization is consistently implementing its ICAM policy, strategy, process, and technology solution road map and is on track to meet milestones. The strategy encompasses the entire organization, aligns with the FICAM and CDM requirements, and incorporates applicable Federal policies, standards, playbooks, and guidelines. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its ICAM policy, strategy, and road map and making updates as needed.	• ICAM roadmap (or other document(s) that shows progress in meeting milestones). • Evidence that lessons learned are incorporated into ICAM policy to improve its effectiveness.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable The organization integrates its ICAM strategy and activities with its enterprise architecture and the Federal ICAM architecture. The organization uses automated mechanisms (e.g., machine-based, or user-based enforcement), where appropriate, to manage the effective implementation of its ICAM policies, procedures, and strategy. Examples of automated mechanisms include network segmentation based on the label/classification of information stored; automatic removal/disabling of temporary/emergency/ inactive accounts; and use of automated tools to inventory and manage accounts and perform segregation of duties/least privilege reviews.	• FICAM segment architecture. • Enterprise architecture. • Documentation supporting the use of automated mechanisms to manage implementation of ICAM policies, procedures, and strategy.
		Optimized On a near real-time basis, the organization actively adapts its ICAM policy, strategy, and related processes and activities to a changing cybersecurity landscape to respond to evolving and sophisticated threats. The organization employs adaptive identification and authentication techniques to assess suspicious behavior and potential violations of its ICAM policies and procedures on a near-real time basis.	• Lessons learned process. • Analysis of the timeliness of updates being made to ICAM policies and procedures relative to changing Federal requirements and guidance and the agency's risk environment.

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
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?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53 (Rev. 5): PS-2 and PS-3 • NIST CSF: PR.IP-11 • OMB M-19-17 • National Insider Threat Policy	FY2024	**Ad Hoc** The organization has not defined its processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems.	
		Defined 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.	• Documentation of agency's established risk designations for granting access. • Documentation describing processes for assigning risk designations for all positions, establishing screening criteria for individuals

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented The organization ensures that all personnel are assigned risk designations, appropriately screened prior to being granted system access, and rescreened periodically.	• Evidence of risk designations assigned to personnel who have access to agency's systems. • Documents or evidence of screening performed on personnel before they are granted access. • Results of periodic screening of personnel who have access to agency's network.
		Managed and Measurable The organization employs automation to centrally document, track, and share risk designations and screening information with necessary parties.	• Documentation supporting the use of automated mechanisms to centrally document, track, and share risk designations and screening information with necessary parties.
		Optimized 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.	• Evidence of the evaluation of personnel security information and related adjustments made. • Request a walkthrough and observe the process of evaluating personnel security information and adjusting permissions.

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized:

29. To what extent does the organization ensure that ***access agreements***, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and nonprivileged users) that access its systems are completed and maintained?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53 (Rev. 5): AC-8, AC-21, CA-3, PL-4, and PS-6	FY2023	**Ad Hoc** The organization has not defined its processes for developing, documenting, and maintaining access agreements for individuals that access its systems.	
		Defined The organization has defined its processes for developing, documenting, and maintaining access agreements for individuals that access its systems.	• ICAM policies and procedures. • Information security program policy. • User access form/ROB/NDA templates (At organization-wide level and, if applicable, division level specific to the system). • Acceptable use policy and method for acknowledgement.
		Consistently Implemented The organization ensures that access agreements for individuals are completed prior to access being granted to systems and are consistently maintained thereafter. The organization uses more specific/detailed agreements for privileged users or those with access to sensitive information, as appropriate.	• Sample of access agreements, rules of behavior, NDAs, for non-privileged and privileged users (at the organization level and if applicable, division level specific to the system). • Screenshots of system use notification for sample internal and external systems.
		Managed and Measurable The organization uses automation to manage and review user access agreements for privileged and non-privileged users. To the extent practical, this process is centralized.	• Screenshots of automated tool or observation of other centralized method to manage access agreements.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Optimized On a near real-time basis, the organization ensures that access agreements for privileged and non-privileged users are maintained, as necessary.	• Alerting function/automation that access agreements need to be refreshed in accordance with agency policy.

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized:

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?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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 800-207 Tenet 6	Core	**Ad Hoc** 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 require strong authentication.	

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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 • EO 14028, Section 3 • OMB M-19-17 • OMB M-22-09 • OMB M-24-04 • CIS Top 18 Security Controls: Control 6 • CISA Capacity Enhancement Guide		**Defined** 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.	• Project plan or policies and procedures for implementation of strong authentication. • E-authentication risk assessment policy and procedures. • Site security plans identifying defined entry/exit points that must be protected.
		Consistently Implemented 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 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.	• Physical access control system configurations identifying strong authentication mechanisms on all defined protected entry/exit points. • E-authentication risk assessments for sample systems. • System security plan for sampled systems. • OS- and Domain-level (Active Directory or similar directory service) configuration settings related to strong authentication. • Mobile device management configuration settings related to strong authentication. • Plans for centralized identity mgt systems. • Phishing resistant MFA • Plans for removal of passwords that require special characters or regular rotation, including in Mobile Device Management solutions.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable 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.	• Review of Active Directory (or similar directory service) configuration setting showing that two-factor is enabled and enforced for all non-privileged users. • Physical access control configurations/documentation demonstrating that all non-privileged users are required to utilize strong authentication mechanisms for entry/exit at defined points.
		Optimized 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.	• Agency documentation of systems that are integrated and support AD/PIV-based login. • Screenshots of automated tools that manages user accounts and privileges and its reporting feature or request a walkthrough and observe the process to manage accounts.

Assessor Best Practices
Defined: **Consistently Implemented:** Test (with a non-privileged user) login without PIV or LOA4 credential and see if access will still be authenticated. Analyze OS- and domain-level configuration settings to determine whether strong authentication is enabled and enforced. **Managed and measurable:** **Optimized:** Select sample systems and test whether AD/PIV-based single sign on is enabled and enforced.

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?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53 (Rev. 5): AC-17 and PE-3 • NIST SP 800-63 • NIST SP 800-128 • NIST SP 800-157 • NIST 800-207 Tenet 6 • NIST CSF: PR.AC-1 and 6 • NIST Security Measures for EO-Critical Software Use: SM 1.1 • FIPS 201-2	Core	**Ad Hoc** 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.	
		Defined 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.	• Project plan for implementation of strong authentication for privileged users. • E-authentication risk assessment policy and procedures. • Site security plans identifying defined entry/exit points that must be protected.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• HSPD-12 • EO 14028, Section 3 • OMB M-19-17 • OMB M-22-09 • OMB M-24-04 • DHS ED 19-01 • CIS Top 18 Security Controls: Control 6		**Consistently Implemented** 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	• Physical access control system configurations identifying strong authentication mechanisms on all defined protected entry/exit points. • Digital identity risk assessments for sample systems. • System security plan for sampled systems. • OS-and domain-level (Active Directory or similar directory service) configuration settings related to strong authentication. • Mobile device management configuration settings related to strong authentication. • Observation of and/or screenshots for sample systems that show how a non-privileged user logs into the network and system. • Plans for centralized identity mgt systems. • Phishing resistant MFA. • Plans for removal of passwords that require special characters or regular rotation, including in Mobile Device Management solutions.
		Managed and Measurable All privileged users, including those who can make changes to DNS records, use strong authentication mechanisms to authenticate to applicable organizational systems.	• Review of AD (or similar directory service) configuration setting showing that two-factor is enabled and enforced for all privileged users. • Physical access control configurations/documentation demonstrating that all privileged users are required to utilize strong authentication mechanisms for entry/exit at defined points.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Optimized 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.	• Agency documentation of systems that support AD/PIV-based login. • Screenshot/Observation of automated tool that manages user accounts and privileges and its reporting feature.

Assessor Best Practices
Defined: **Consistently Implemented:** Test (with a privileged user) login without PIV or LOA4 credential and see if access will still be authenticated. Analyze OS- and domain-level configuration settings to determine whether strong authentication is enabled and enforced. **Managed and measurable:** **Optimized:** Sample select systems and test whether AD/PIV-based login is enabled and enforced as well as physical access controls.

32. To what extent does the organization ensure that ***privileged accounts are provisioned, managed, and reviewed*** in accordance with the principles of least privilege and separation of duties? *Specifically*, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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 • EO 14028, Section 8 • OMB M-19-17 • OMB M-21-31 • DHS ED 19-01 • CIS Top 18 Security Controls: Controls 5, 6, and 8	Core	**Ad Hoc** The organization has not defined its processes for provisioning, managing, and reviewing privileged accounts.	
		Defined 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.	• ICAM policies and procedures to include privileged accounts. • Audit logging policies and procedures to include privileged accounts. • Access control policies and procedures addressing separation of duties and least privilege requirements.
		Consistently Implemented 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.	• Observation/documentation of domain, operating system, and network device account settings for privileged accounts. • Log review reports for privileged user accounts. • Inventory of privileged user accounts by type. • List of auditable events for privileged users by system type. • List of users by type and role for sampled systems. • Controls that limit the duration a privileged user can be logged in. • Controls that limit the privileged functions during remote access.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable 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.	• Screenshots of automated tool or other mechanism that shows the management of privileged accounts and the automatic removal/disabling of temporary/emergency/inactive accounts.
		Optimized The organization is making demonstrated progress towards implementing EL3's advanced requirements for user behavior monitoring to detect and alert on privileged user compromise.	• Evidence of EL3 requirements for user behavior monitoring. • Examples of alerts of privileged user compromises.

Assessor Best Practices
Defined: **Consistently Implemented:** Review the roles and responsibilities of stakeholders involved in the agency's ICAM activities and identify those that require separation of duties to be enforced (e.g., information system developers and those responsible for configuration management process). Ensure that the principle of separation of duties is enforced for these roles. **Managed and measurable:** **Optimized:**

33. To what extent does the organization ensure that appropriate ***configuration/connection requirements are maintained for remote access connections***? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-46 (Rev. 2) • NIST SP 800-53 (Rev. 5): AC-11, AC-12, AC-17, AC-19, AU-2, IA-7, SC-10, SC-13, and SI-4 • NIST CSF: PR.AC-3	FY2023	**Ad Hoc** The organization has not defined the configuration/connection requirements for remote access connections, including use of FIPS 140- 2 validated cryptographic modules, system time-outs, and monitoring and control of remote access sessions.	
		Defined The organization has defined its configuration/connection requirements for remote access connections, including use of cryptographic modules, system time-outs, and how it monitors and controls remote access sessions.	• Remote access policies and procedures. • Audit logging policies and procedures.
		Consistently Implemented The organization ensures that FIPS 140-2 validated cryptographic modules are implemented for its remote access connection method(s), remote access sessions time out after 30 minutes (or less), and that remote users' activities are logged and reviewed based on risk.	• Configuration of VPN solution and settings for system timeouts and encryption. • List of auditable events for remote access solution. • Encryption cert for VPN server/browser settings. • Log review report for remote access connections.
		Managed and Measurable The organization ensures that end user devices have been appropriately configured prior to allowing remote access and restricts the ability of individuals to transfer data accessed remotely to non-authorized devices.	• Configuration of DLP or other mechanism preventing transfer of data to non-authorized devices. • Documentation of the checks performed on host systems prior to remote connection.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Optimized The organization has deployed a capability to rapidly disconnect remote access user sessions based on active monitoring. The speed of disablement varies based on the criticality of missions/business functions.	• Over-the-shoulder' demonstration of how a connection exhibiting inappropriate behavior is monitored for, detected, and rapidly disconnected. • Other artifacts supporting the deployment of this capability which could include, for example, logs showing examples of the disconnection of connections as a result of active monitoring.

Assessor Best Practices

Defined:

Consistently Implemented: Evaluate the agency's ability to disconnect remote access sessions in a timely fashion based on potential malicious activity or abnormal behaviors on the network. Such activity could include unauthorized/large data transfers, etc.

Managed and measurable:

Optimized:

34. Provide any additional information on the effectiveness (positive or negative) of the organization's ***identity and access management program*** that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
	Annual	**Ad Hoc**	•
		Defined	•
		Consistently Implemented	•

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable	•
		Optimized	•

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized:

Data Protection and Privacy (DPP)

35. To what extent has the organization ***developed a privacy program*** for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-37 (Rev. 2): Section 2.3 and Task P-1 • NIST SP 800-53, Rev. 5: CA-2, RA-3, RA-8, SA-8(33), PM-5(1), PM-20, PM-27, PT-5, PT-6, and SI-12(1) • NIST SP 800-122 • CSF: ID.GV-3 • NIST Privacy Framework • OMB M-19-03	FY2023	**Ad Hoc** The organization has not established a privacy program and related plans, policies, and procedures as appropriate for the protection of PII collected, used, maintained, shared, and disposed of by information systems. Additionally, roles and responsibilities for the effective implementation of the organization's privacy program have not been defined.	

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• OMB M-20-04 • OMB A-130 • FY 2022 SAOP FISMA Metrics: Sections 1, 4, and 5(b)		**Defined** The organization has defined and communicated its privacy program plan and related policies and procedures for the protection of PII that is collected, used, maintained, shared, and/or disposed of by its information systems. In addition, roles and responsibilities for the effective implementation of the organization's privacy program have been defined and the organization has determined the resources and optimal governance structure needed to effectively implement its privacy program.	• Privacy program strategy/plan for implementing applicable privacy controls policies and procedures • Privacy policies and procedures related to protection of PII on information systems • Privacy program organizational chart, budget, reporting structure, roles and responsibilities, etc.
		Consistently Implemented The organization consistently implements its privacy program by: • Dedicating appropriate resources to the program • Maintaining an inventory of the collection and use of PII • Conducting and maintaining privacy impact assessments and system of records notices for all applicable systems • Reviewing and removing unnecessary PII collections on a regular basis (i.e., SSNs) • Using effective communications channels for disseminating privacy policies and procedures • Ensuring that individuals are consistently performing the privacy roles and responsibilities that have been defined across the organization	• Staffing vacancies in the privacy program • Interviews with privacy program staff regarding resource sufficiency • PII Inventory (the types of PII records maintained by system and their sources) • PIAs and SORNs • PII reviews • Plans and/or procedures to remove unnecessary PII

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable The organization monitors and analyses quantitative and qualitative performance measures on the effectiveness of its privacy activities and uses that information to make needed adjustments. The organization conducts an independent review of its privacy program and makes necessary improvements.	• Privacy activities performance measure reports/dashboards • Evidence that the agency incorporates performance measures feedback to make appropriate adjustments as needed.
		Optimized The privacy program is fully integrated with other security areas, such as ISCM, and other business processes, such as strategic planning and risk management. Further, the organization's privacy program is embedded into daily decision making across the organization and provides for continuous identification of privacy risks.	• ISCM strategy • Strategic planning documents • Risk management strategy • Incident response plans • Cyber threat information sharing policies/procedures. • Report from independent review of the privacy program

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
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

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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 800-207 • 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 2.4 • OMB M-22-09 • DHS BOD 18-02 • CIS Top 18 Security Controls v. 8: Control 3	Core	**Ad Hoc** The organization has not defined its policies and procedures in one or more of the specified areas.	
		Defined 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.	• Information security, data life cycle, and/or protection policies and procedures • Data classification/handling policies and procedures • Destruction/sanitization policies and procedures
		Consistently Implemented 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.	• Evidence of database, file share, server, and/or end point encryption where PII or sensitive information is stored. • Evidence of use of SSL/TLS across external communication boundaries • Evidence of capability to communicate PII or sensitive information internally (e.g., email encryption) • Evidence/testing of network access controls or other methods used to prevent and detect untrusted removable media • Evidence of destruction/sanitization
		Managed and Measurable 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.	• ISCM strategy • Continuous monitoring reports and evidence of review of applicable privacy controls

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Optimized 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.	• Documentation of agency use of remote wiping for agency devices • Evidence of dual authorizations for sanitization of devices that contain sensitive information • Data dictionary for systems containing PII, highlighting the fields used to record PII collection • Evidence of data storage/destruction in accordance with the data retention schedule

Assessor Best Practices
Defined:
Consistently Implemented: Encryption algorithms used to encrypt data at rest and in transit must be FIPS-validated.
Managed and measurable:
Optimized:

37. To what extent has the organization implemented security controls (e.g., EDR) to ***prevent data exfiltration*** and enhance network defenses?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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	Core	**Ad Hoc** 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.	

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST Security Measures for EO-Critical Software Use: SM 4.3 • OMB M-21-07 • OMB M-22-01 • CIS Top 18 Security Controls v.8: Controls 9 and 10 • DHS BOD 18-01 • DHS ED 19-01		**Defined** 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.	• Data exfiltration/network defense policies and procedures
		Consistently Implemented 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 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.	• Evidence of web content filtering tools to monitor inbound and outbound traffic for phishing, malware, and domain filtering • Evidence of DLP used to monitor outbound traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII • Evidence that suspected malicious traffic is quarantined/blocked. • Evidence of email authentication utilization • DNS records audit results • Evidence of valid domain encryption certificates

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable 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 gaps, and is coordinating with CISA for future EDR solution deployments.	• Data exfiltration and network defense performance measure reports/dashboards • After-action reports/meeting minutes from exfiltration exercises • Evidence that DNS infrastructure is monitored in accordance with ISCM strategy
		Optimized 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.	• ISCM strategy • Incident response plan • Evidence showing integration with other security domains, including configuration management, ISCM, and incident response

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized:

38. To what extent has the organization developed and implemented a ***Data Breach Response Plan***, as appropriate, to respond to privacy events?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53 (Rev. 5): IR-8 and IR-8(1) • NIST SP 800-122 • OMB M-17-12 • OMB M-24-04 • FY 2022 SAOP FISMA Metrics: Section 12	FY2024	**Ad Hoc** 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.	
		Defined 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.	• Data Breach Response Plan that includes the agency's policies and procedures for reporting, investigating, and managing a breach exists and is tailored to the agency. • Evidence of an established Breach Response Team including the specific agency officials that comprise the team as well as their respective roles and responsibilities in responding to a breach. • Evidence that the Data Breach Response Plan was formally approved by the SAOP and communicated to the agency.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented 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.	• Evidence/Observation of table-top exercises • Evidence of After-Action Report/Lessons Learned • Evidence of updates to the Breach Response Plan based on lessons learned (if applicable). • Evidence the agency is using General Services Administration's (GSA) identity protection services (IPS) blanket purchase agreements (BPAs) for identity monitoring, credit monitoring, and other related services.
		Managed and Measurable 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.	• Evidence of Breach Response qualitative and quantitative metrics were collected. • Templates to support that Breach Response Data was obtained accurately, consistently, and in a reproduceable format.
		Optimized 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.	• Evidence of automated tools such as Data Loss Prevention Tools • Automated monitoring of system logs for unusual activity

Assessor Best Practices
Defined: The Assessor should review the Breach Response Plan to ensure it contains the agency's policies and procedures for reporting, investigating, and managing a breach and is tailored to the agency. In addition, the Assessor should ensure the Breach Response Plan includes the minimum elements required by OMB M-17-12, Section VII. The Assessor should determine whether the Agency established a Breach Response Team that consists of a group of agency officials designated by the head of the agency to convene to respond to a breach. Does the Breach Response Team include the SAOP, the CIO or the CIO's designee, Senior Agency Information Security Officer, Legal counsel, Legislative affairs official, and a Communications official? **Consistently Implemented:** The Assessor should observe or review results from the most recent tabletop exercise conducted by the Breach Response Team. Did the Breach Response Team conduct the tabletop exercise at least annually? Did the exercise test the breach response plan to ensure that members of the team are familiar with the plan and understand their specific roles? Did the tabletop exercise identify potential weaknesses in an agency's response capabilities that resulted in improvements to the Breach Response Plan? Does the Agency use GSA's identity protection services (IPS) blanket purchase agreements (BPAs) for identifying monitoring, credit monitoring, and other related services? **Managed and measurable:** The Assessor should determine whether the Agency developed a formal process to track and document each breach reported to the agency. Does the Agency use a breach reporting template (as required by OMB M-17-12) to track and monitor the total number of breaches over time, the status for each reported breach, the number of individuals potentially affected by each reported breach, the types of information potentially compromised by each reported breach, whether the agency notified individuals potentially affected by the breach, whether the agency provided services to the individuals affected by a breach, and whether the breach was reported to US-CERT or Congress. **Optimized:** The Assessor should review whether the breach response plan integrates with Agency risk management, incident response, continuous monitoring, continuity of operations, and other mission/business areas. Does the agency use any automated tools, such as Data Loss Prevention or Security Information and Event Management, to identify and monitor for potential privacy incidents? Do any of the tools offer automated alerting of privacy events?

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.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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	FY2024	**Ad Hoc** 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.	
		Defined 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.	• Privacy awareness training program strategy/plan. • Security training policies and procedures are tailored to the agency's mission and risk environment.
		Consistently Implemented 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.	• Completion records for basic privacy awareness training. • Completion records for role-based privacy training for certain staff with PII responsibilities. • Signed acceptance/attestation records of responsibility for privacy requirements.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable 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.	• Evidence of an automated tracking system designed to capture key information regarding training activity (e.g. courses, dates, audiences, costs, sources). • Evidence of evaluation and feedback mechanisms to improve the training program. • Evidence of targeted phishing exercises for those with responsibility for PII and exercise results. • Evidence of review and updates to the training program.
		Optimized The organization has institutionalized a process of continuous improvement incorporating advanced privacy training practices and technologies.	Intentionally Blank

Assessor Best Practices
Defined: Does the Agency have a privacy awareness training program strategy or plan that includes requirements for role based privacy awareness training? Has the training strategy or plan been communicated to the agency? Is the training program tailored to the agency's mission and risk environment? **Consistently Implemented:** The Assessor should determine how the organization ensures all individuals receive basic privacy awareness training. What percentage of the agency's Federal employees (including managers and senior executives) received foundational privacy training during the annual reporting period? Does the Agency provide role-based privacy training to its Federal employees with assigned privacy roles and responsibilities? What percentage of the agency's Federal employees with assigned privacy roles received role-based training during the annual reporting period? The Assessor should determine whether the Agency established rules of behavior, including consequences for violating rules of behavior, for employees and contractors that have access to Federal information or information systems. Does the Agency require employees and contractors to certify acceptance of their responsibilities for privacy requirements at least annually? The Assessor should obtain evidence of the annual certification of acceptance. **Managed and measurable:** Determine how the agency measures the effectiveness of its privacy awareness training program. Does the agency have a process for obtaining feedback on the content of the training? Does the agency conduct targeted phishing exercises for those with

responsibility for PII? Have there been any audits or internal assessments of the privacy training program? If so, what updates did the agency make based on those reviews?

Optimized: The Agency maintains an ongoing awareness of privacy risks and assesses privacy controls to ensure compliance with applicable privacy requirements and to manage privacy risks. The agency maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks and updates privacy training practices and technologies as needed.

40. Provide any additional information on the effectiveness (positive or negative) of the organization's ***data protection and privacy program*** that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
	Annual	**Ad Hoc**	•
		Defined	•
		Consistently Implemented	•
		Managed and Measurable	•
		Optimized	•

Assessor Best Practices

Defined:

Consistently Implemented:

Managed and measurable:

Optimized:

Security Training (ST)

41. To what extent have the ***roles and responsibilities*** of security awareness and training program stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?

Note: This includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-50 • NIST SP 800-53 (Rev. 5): AT-1 • Green Book: Principles 3, 4, and 5	FY2023	**Ad Hoc** Roles and responsibilities have not been defined, communicated across the organization, and appropriately resourced.	
		Defined Roles and responsibilities have been defined and communicated across the organization and resource requirements have been established.	• Information security program policy, including roles and responsibilities. • Security awareness and training policies and procedures
		Consistently Implemented Individuals are performing the roles and responsibilities that have been defined across the organization.	• IT and cyber training budget established for agency-wide security awareness and role-based training • Review the independent assessment of the AT-1(b) and AT-1(c) security control across organization. Assessment determines whether organization designates key training roles and reviews/updates training. • Current organization chart showing whether roles are filled.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to consistently implement security awareness and training responsibilities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	• Evidence that the Agency tracks security training to ensure training completion and accountability, including the tracking and monitoring of individual training completion; • Evidence training resources prioritize high trust/high impact positions; • Evidence the central security training authority has a strategy for policy and program requirement enforcement;
		Optimized The organization continuously evaluates and adapts its security training roles and responsibilities to account for a changing cybersecurity landscape.	• Evidence showing training has been tailored to different audiences and is regularly updated, including agency specific risks and persistent threats (risk profile); • Evidence of correlation between incident response and security training content; • Established qualitative or quantitative metrics to ensure the effectiveness of the training program and using that information to make continuous program improvements.

Assessor Best Practices
Defined: Determine the structure of the Agency Awareness and Training Program (NIST SP 800-50, section 3.1) to understand information dissemination, resource allocation, and responsibilities. Assessors should verify the organizational security training program assigns essential security training roles and responsibilities in accordance with NIST SP 800-50, Section 1.5. In addition, funding sources for the program are well defined. **Consistently Implemented:** Assessors should determine if staff with security roles received role-based training tailored to their positions by assessing the effectiveness of NIST 800-53rev5 control AT-1 "Policy and Procedures". Additionally, assessors should utilize a survey or questionnaire to determine if vacancies exist in defined security training roles across the Agency (e.g., CISO, ISSO, IT Security Staff). **Managed and measurable:** Assessors determine if metrics, measurements, or any other analytical data has been developed to ensure staff in relevant security roles are performing required duties. **Optimized:** Assessors should review evidence that supports the organization has tailored its security awareness trainings for different audiences. Additionally, assessors review whether such trainings are regularly updated to reflect the latest threats. (e.g., uptake in phishing incidents leads to increasing phishing content in role-based trainings).

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?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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	Core	**Ad Hoc** The organization has not defined its processes for assessing the knowledge, skills, and abilities of its workforce.	
		Defined 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.	• Workforce assessment policies and procedures (or related documentation) • Security training policies and procedures

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• National Cybersecurity Workforce Framework • CIS Top 18 Security Controls: Control 14 • EO 13870		**Consistently Implemented** 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.	• Cybersecurity Workforce assessment considers the agency's risk profile and includes any relevant skill gaps • Content of awareness and role-based training programs • Action plan to close gaps identified through its workforce assessment • Training Strategy/Plan(s) tailored by workforce assessment
		Managed and Measurable The organization has addressed its identified knowledge, skills, and abilities gaps through training or talent acquisition.	• Evidence that the Agency measures workforce/KSA needs, including qualitative or quantitative metrics to ensure the effectiveness of the training program • Evidence of training and talent acquisition to address identified needs and skill gaps
		Optimized 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.	• Evidence of trend analysis performed showing incidents attributable to personnel actions or inactions being reduced over time • Evidence that the awareness and specialized (role based) training programs are effective and the agency is making continuous program improvements.

Assessor Best Practices
Defined: Assessors reviews policies and procedures related to workforce assessments and staffing plans to ensure that the agency has established methods to assess its own security capabilities and needs. Agency models policies and procedures based on NICE Framework. **Consistently Implemented:** Assessors reviews evidence showing the Agency has assessed the KSAs of their cybersecurity workforce and the assessment utilizes the NICE Framework. Additionally, Agency integrates newly emerging security threats into security training by assessing effectiveness of NIST 800-53r5 security control AT-2(c) and AT-2(d) "Literacy Training and Awareness." **Managed and measurable:** Assessors review evidence showing that workforce assessments have been collected and has been used to inform future strategies. Assessors also examine whether training and talent acquisition utilize workforce assessments to fill gaps. **Optimized:** Assessors review evidence to determine whether the Agency can attribute positive security trends to prior workforce training. Examples: tracking the success of phishing exercises and number of user-submitted phishing notifications against phishing and security awareness training, or a positive trend in SOC metrics due to workforce KSA improvement.

43. To what extent does the organization ***use a security awareness and training strategy/plan*** that leverages its skills assessment and is adapted to its mission and risk environment?

Note: The strategy/plan should include the following components:

- The structure of the awareness and training program
- Priorities
- Funding
- The goals of the program
- Target audiences
- Types of courses/ material for each audience
- Use of technologies (such as email advisories, intranet updates/wiki pages/social media, web-based training, phishing simulation tools)
- Frequency of training
- Deployment methods

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-50: Section 3 • NIST SP 800-53 (Rev. 5): AT-1 • NIST CSF: PR.AT-1 • OMB M-16-15	FY2023	**Ad Hoc** The organization has not defined its security awareness and training strategy/plan for developing, implementing, and maintaining a security awareness and training program that is tailored to its mission and risk environment.	
		Defined The organization has defined its security awareness and training strategy/plan for developing, implementing, and maintaining a security awareness and training program that is tailored to its mission and risk environment.	• Security awareness training programs strategy/plan • Security training policies and procedures are tailored to the agency's risk profile and persistent threats

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented The organization has consistently implemented its organization-wide security awareness and training strategy and plan.	• Completion records for security awareness and role-based training • Cybersecurity Workforce Assessment and associated gap analysis
		Managed and Measurable The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	• Evidence of an automated tracking system designed to capture key information regarding program activity (e.g., courses, dates, audiences, costs, sources), including qualitative or quantitative metrics to ensure the effectiveness of the training program • Evidence of evaluation and feedback mechanisms to continuously improve the program
		Optimized The organization's security awareness and training activities are integrated across other security-related domains. For instance, common risks and control weaknesses, and other outputs of the agency's risk management and continuous monitoring activities inform any updates that need to be made to the security awareness and training program.	

Assessor Best Practices
Defined: IG assessor confirms the organization has developed and disseminated a security policy and plan and confirms whether the plan was tailored for the Agency mission(s) or risk tolerance.

Consistently Implemented: IG assessor analyzes the Agency security awareness and training program to determine if the program implements the following components:

- The structure of the awareness and training program
- Priorities
- Funding
- The goals of the program
- Target audiences
- Types of courses/ material for each audience
- Use of technologies (such as email advisories, intranet updates/wiki pages/social media, web-based training, phishing simulation tools)
- Frequency of training
- Deployment methods

Managed and measurable: IG assessors assess analytical evidence (e.g., charts, graphics, and other output) that supports the organization has used metrics in place to measure effectiveness if security training program and has produced repeatable output. Additionally, obtain evidence that the organizational collects user feedback based on trainings.

Optimized: IG assessor should assess whether security awareness and training activities integrate with Agency risk management and continuous monitoring activities.

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?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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	FY2024	**Ad Hoc** 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.	

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Defined The organization has defined and tailored its security awareness policies, procedures, and related material and delivery methods based on FISMA requirements, its mission, risk environment, 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.	• Security awareness policies and procedures that include processes for ensuring all system users (including contractors) are provided security awareness training. • Security awareness policies and procedures include a defined timeframe for initial training and periodically thereafter. • Security awareness policies and procedures are tailored to the agency. • Policy or procedures contain process(es) for evaluating and obtaining feedback on the security awareness training program.
		Consistently Implemented 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.	• Completion records for security awareness training. • Evidence all new users (including contractors) completed training within defined timeframes. • Evidence all users completed training periodically as defined in policy. • Evidence of the design and implementation of a feedback strategy.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
Same Previous List	FY2024	**Managed and Measurable** 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.	• Evidence of phishing exercises and results of those exercises. • Evidence of additional training provided, or disciplinary action taken, as appropriate. • Evidence that the agency monitors performance measures on the effectiveness of its security awareness policies, procedures, and practices. • Review evidence and artifacts to determine whether data supporting metrics are obtained accurately, consistently, and in a reproducible format, such as using dashboards or automated tools/reporting mechanisms.
Same Previous List	FY2024	**Optimized** 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.	• Evidence of ongoing review and updates to the security awareness program.

Assessor Best Practices
Defined: Determine whether the agency IT security program policy includes a distinct section devoted to agency wide requirements for the awareness and training program (NIST SP 800-50, Section 1.4). Determine whether the agency developed IT security awareness training policy and procedures for ensuring all system users (including contractors) are provided security awareness training and the agency has defined the timeframe for initial training and periodically thereafter. Is the awareness training tailored to the agency? Does agency policy and procedures identify processes for evaluating and obtaining feedback on the security awareness and training program? **Consistently Implemented:** Determine whether the agency has an automated tracking system to capture key information regarding the security awareness and training program. Assessors should review evidence to determine whether all new users completed training within the timeframe defined in policy and all users completed training periodically, as defined in agency policy. Did the agency track compliance to assess the status of the training program or generate reports to identify gaps or problems with the training program? What methods did the agency use to solicit feedback? **Managed and measurable:** The assessor should obtain evidence and results of phishing exercises or other methods used by the agency to measure the effectiveness of the awareness program. Does the agency have sufficient funding to implement their awareness training strategy? Does the agency use metrics to identify gaps or to adapt its security awareness policies, procedures, or processes? The Assessor should look for examples of corrective action or necessary follow-up based on results of metrics or management information reports. Follow-up action could include formal reminders to management; additional awareness, training, or education offerings; and/or the establishment of a corrective plan with scheduled completion dates. **Optimized:** Determine whether the CIO, program officials, and IT security program managers advocate for continuous improvement and support of the agency's security awareness program. Does the agency have a defined set of metrics and automated systems to support the capture of quantitative data and delivery of management information to accountable parties on a regular, predefined cycle? Are Agency monitoring, follow-up, and corrective procedures well defined and seamless?

45. To what extent does the organization ensure that ***specialized security training*** is provided to individuals with significant security responsibilities (as defined in the organization's security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301)?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53 (Rev. 5): AT-3 and AT-4 • EO 13870 • 5 Code of Federal Regulation 930.301	FY2024	**Ad Hoc** The organization has not defined its security training policies, procedures, and related 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.	
		Defined The organization has defined its security training policies, procedures, and related material based on FISMA 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.	• Evidence of security training policies, procedures, and related material. • Evidence the agency identified personnel with security roles and responsibilities and identified specialized training requirements and frequency.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented The organization ensures that its security training policies and procedures are consistently implemented. 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.	• Evidence of training records for those with significant security responsibilities. • Training completion certificates or other documentation used to record specialized training for individuals with significant security responsibilities.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable The organization obtains feedback on its specialized security training content and processes and makes updates 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.	• Evidence of feedback on the content of specialized training and updates to the program based on feedback, as appropriate. • Evidence of targeted phishing or other exercises to Senior Executives, privileged users, and/or cybersecurity personnel and results of those exercises. • Evidence of additional training offered, or disciplinary action taken, as appropriate. • Evidence that the agency monitors performance measures on the effectiveness of its security awareness policies, procedures, and practices. • Review evidence and artifacts to determine whether data supporting metrics are obtained accurately, consistently, and in a reproducible format, such as using dashboards or automated tools/reporting mechanisms.
		Optimized The organization has institutionalized a process of continuous improvement incorporating advanced 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.	• Evidence the Agency adapts its specialized training policies, procedures, and processes to address a changing threat and technology landscape.

Assessor Best Practices
Defined: Determine whether the agency developed security training policies and procedures based on its mission and risk environment and the types of roles with significant security responsibilities. Do agency policies and procedures identify roles and responsibilities that may require role-based training? Do the agency policies and procedures define the timeframes for completing specialized security training and periodically thereafter? The Assessor should ensure that the policies and procedures also include the process(es) for ensuring personnel with significant security responsibilities receive specialized security training. **Consistently Implemented:** The Assessor should obtain evidence of training records for those with significant security responsibilities. The Assessor may request training completion certificates or other documentation used to record specialized training for individuals. The Assessor should determine whether the content of the specialized training completed matches the individuals' role. The Assessor should review how the agency monitors training for those with significant security responsibilities and mechanisms in place for obtaining feedback on its training program. **Managed and measurable:** The Assessor should obtain evidence of feedback on the content of specialized security training and review any updates to the program based on feedback. The Assessor should obtain evidence of the qualitative and quantitative performance measures the Agency uses to monitor the effectiveness of its security training policies, procedures, and practices and review evidence and artifacts to support those metrics. Did the Agency conduct targeted phishing exercises to Senior Executives, privileged users, and/or cybersecurity personnel to ensure they understand their roles and responsibilities? What actions did the Agency take based on the results of those exercises? For example, did the Agency follow-up with additional training or disciplinary action, as appropriate? **Optimized:** Determine whether the Agency adapts its specialized training policies, procedures, and processes through a process of continuous improvement incorporating the changing threat and technology landscape.

46. Provide any additional information on the effectiveness (positive or negative) of the organization's ***security training program*** that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the security training program effective?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
	Annual	**Ad Hoc**	•
		Defined	•

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented	•
		Managed and Measurable	•
		Optimized	•

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized:

Information Security Continuous Monitoring (ISCM)			
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?			
Criteria	**Review Cycle**	**Maturity Level**	**Suggested Standard Source Evidence**
• 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	**Ad Hoc** The organization has not developed, tailored, and communicated its ISCM policies and an organization wide ISCM strategy.	
		Defined 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 criterion for determining minimum frequencies is established in coordination with organizational officials [e.g., senior accountable official for risk management, system owners, and common control 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.	• ISCM strategy, including evidence that the strategy was developed for selected systems. • ISCM policies and procedures • Agency-wide information security policy • List of approved continuous monitoring tools and technologies

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented 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 improvements to the ISCM policies and strategy.	• Continuous monitoring reports, or other assessment products, for selected systems • Evidence that agency dashboard is fully functional with visibility of all organizational assets • Evidence of an ongoing lessons learned process
		Managed and Measurable 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 continuous monitoring policies and strategy.	• Evidence of ongoing performance metrics/dashboards as defined in the ISCM strategy • Evidence of verifications/validation of data feeding the metrics/dashboard • Evidence of control assessments performed at frequency defined by ongoing assessment strategy/schedule. • Evidence of system authorizations for select systems (including OSA schedules, POA&Ms, SSPs, SARs, and ATO letters)

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Optimized 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.	• Evidence supporting continuous monitoring tools and technologies are used in other security domains, including risk management, configuration management, incident response, and business continuity.

Assessor Best Practices

Defined: Review the organization-wide ISCM strategy and confirm the strategy has defined (1) the frequency at which organizational systems will be assessed, (2) how ongoing assessments will be carried out and at what frequency, and (3) a risk-based approach supporting security control assessment frequency selection.

Consistently Implemented: Review evidence (e.g., reports or analysis output from an agency dashboard) that support control assessments occur on an ongoing basis and continuous monitoring (e.g., known vulnerabilities, patches, etc.) at all three levels: organization, business process, and information system. Additionally, obtain and review agency dashboard screenshots (e.g., CDM or agency dashboard and/or SIEM etc.) that support the organization's visibility over the asset and vulnerabilities. Lastly, review reports or other analysis, including shareholders feedback that is utilized to create lessons learned.

Managed and measurable: Ensure the organization has (1) defined qualitative and quantitative performance metrics within its ISCM plan and that they have used them to produce reports and other output for review, (2) evidence (e.g., assessment results) that support control assessments occur on the ongoing basis defined in the systems ISCM strategy, and (3) evidence that authorization decisions are based on the results of ongoing assessments.

Optimized: Ensure the outputs of the ISCM process serve as inputs to the agency's risk management, incident response, business continuity, configuration management, and other related programs on a near-real time basis.

48. To what extent have ISCM stakeholders and their ***roles, responsibilities, levels of authority, and dependencies*** been defined, communicated, and implemented across the organization?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-37, Rev. 2: Tasks P-7 and S-5 • NIST SP 800-53 (Rev. 5): CA-1 • NIST SP 800-137 • NIST CSF: DE.DP-1 • Green Book: Principles 3, 4, and 5	FY2023	**Ad Hoc** Roles and responsibilities have not been fully defined and communicated across the organization, including appropriate levels of authority and dependencies.	
		Defined The organization has defined and communicated the structures of its ISCM team, roles and responsibilities of ISCM stakeholders, and levels of authority and dependencies.	• Information security program policy • ISCM strategy, policies, and procedures • Organizational charts • Delegations of authority • Defined roles and responsibilities
		Consistently Implemented Individuals are performing the roles and responsibilities that have been defined across the organization.	• Evidence that individuals that are assigned the ISCM defined roles are carrying out their responsibilities at all levels (organization, business process, and information system) • Agency's IT security budget • Interviews with system security staff

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement ISCM activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	• Evidence of use of performance metrics/dashboards defined in the ISCM strategy • Evidence of verifications/validation of data feeding the metrics/dashboard • Evidence of coordination amongst other related security domains. • Evidence that individuals with ISCM responsibilities are held accountable (e.g., performance rating templates or similar documentation)
		Optimized The organization continuously evaluates and adapts its ISCM-based roles and responsibilities to account for a changing cybersecurity landscape.	• Evidence that input/knowledge/guidance/lessons learned from oversight agencies (DHS, OMB, CISA, etc.) are being incorporated into decision making for ISCM resource allocation.

Assessor Best Practices

Defined: Review the ISCM plan and ensure the organization has defined roles and responsibilities related to ISCM.

Consistently Implemented: Assessor should review (1) organizational charts and ensure defined roles are filled, and (2) organizations IT security budget to ensure it assesses gaps and vacancies and perform interviews with staff to determine if ISCM is adequately resourced.

Managed and measurable: Assessor should evaluate whether the organization has defined metrics to assess ISCM performance roles and ensure individuals with roles have been assessed.

Optimized: Assessor should ensure evidence shows that strategies, policies, procedures, and input from oversight agencies are being implemented and incorporated into ISCM decision making.

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?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-18 • 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	Core	**Ad Hoc** 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, and monitoring security controls for individual systems and time-based triggers for ongoing authorization.	
		Defined 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, and 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.	• ISCM strategy • Assessment schedules • ISCM policies and procedures • Agency-wide information security policy

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented 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.	• Evidence of ongoing security control assessments for a sample of systems at the appropriate level of rigor and frequency • Evidence of system authorizations for select systems (including OSA schedules, POA&Ms, SSPs, SARs, and ATO letters) • Organization-wide risk management strategy, appetite, and tolerance
		Managed and Measurable The organization utilizes 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.	• Evidence of the generation and collection of security-related information for all implemented security controls, including inherited common controls, at the frequencies specified in the ISCM strategy

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Optimized 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.	• See assessor best practices below

Assessor Best Practices
Defined: Evaluate the agency's ISCM procedures to see whether they include risk determinations and risk acceptance decisions taken at agreed-upon and documented frequencies in accordance with the organization's mission/business requirements and risk tolerance. For moderate and high impact systems, evaluate whether the security-related information provided to the Authorizing Official to support ongoing authorization is produced/analyzed by an independent entity. **Consistently Implemented:** **Managed and measurable:** **Optimized:** Ensure automated tools are used to the extent practicable to support authorizing officials in making ongoing authorization decisions. In cases where automation is not feasible, manual or procedural security assessments are conducted to cover the gaps.

50. How mature is the organization's process for collecting and analyzing ***ISCM performance measures*** and reporting findings?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-137	FY2024	**Ad Hoc** 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 organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions.	
		Defined 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 format of reports, frequency of reports, and the tools used to provide information to individuals with significant security responsibilities.	• ISCM performance measures • Evidence of management dashboards that support reporting functionality.
		Consistently Implemented 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.	• Screenshots or demo of organization-wide ISCM dashboards. • Reports generated from the tool that captures performance measures. • POA&Ms and reports as a result of an ISCM assessment and/or system authorizations.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable 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 operations and security domains.	• ISCM dashboards feeding into other areas of information security. • Reports with visibility across the organization.
		Optimized 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.	• Evidence of automation to capture, correlate, analyze and report the overall security status of the organization.

Assessor Best Practices

Defined: A security management dashboard (or security information management console) consolidates and communicates information relevant to the organizational security status in near real-time to security management stakeholders. Personnel with responsibility for information security range from a technical system administrator, to the CISO, to the risk executive (function).

Consistently Implemented: The security management dashboard presents information in a meaningful and easily understandable format that can be customized to provide information appropriate to those with specific roles and responsibilities within the organization. To maximize the benefits of management dashboards, it is important to obtain acceptance and support from upper-level management, define useful and quantifiable organization-specific performance metrics that are based on information security policies and procedures, and ensure the availability of meaningful performance data.

Managed and measurable: The implementation and effective use of management dashboards can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800- 53 security controls including AC-5, Separation of Duties; CA-6, Security Authorization, CA-7, Continuous Monitoring; PM-6, Information Security Measures of Performance; PM-9, Risk Management Strategy; RA-3, Risk Assessment; and SI-4, Information System Monitoring.

Optimized: Automation is an efficient way to enable ISCM within and across domains to capture, correlate, analyze, and report the overall security status of the organization. Automation specifications and standardized formats enable the interoperability and flow of data between these domains. Just about every security tool provides some sort of automated capability as part of its functionality, including importing and exporting data and performing other pre-configured, unassisted operations. Some of these automated capabilities rely on proprietary methods and protocols,

while others use standardized specifications and methods. When using a tool that automatically configures devices or changes settings, the new configurations are first tested in a test environment. Some examples of security automation activities include:

- Scanning for vulnerabilities and automatically applying the appropriate patches;
- Automatically enabling security configurations based on a checklist of security settings;
- Scanning for compliance against a pre-configured checklist of security settings; and
- Collecting security metrics from tools and reporting them to a management console in a standardized format.

51. Provide any additional information on the effectiveness (positive or negative) of the organization's ***ISCM program*** that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
	Annual	**Ad Hoc**	•
		Defined	•
		Consistently Implemented	•
		Managed and Measurable	•
		Optimized	•

Assessor Best Practices

Defined:

Consistently Implemented:

Managed and measurable:

Optimized:

Incident Response (IR)

52. To what extent does the organization ***use an incident response plan*** to provide a formal, focused, and coordinated approach to responding to incidents?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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 8: National Preparedness | Homeland Security (dhs.gov)	FY2024	**Ad Hoc** The organization has not developed an incident response plan to provide a roadmap for implementing its incident response capability.	
		Defined 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	• Agency incident response plan • Incident response policies and procedures
		Consistently Implemented 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.	• Examples of reportable incidents • After action reports containing lessons learned • Examples of updating the IR plan

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable 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.	• Metrics defined in the IR plan • Evidence of how this data is captured
		Optimized 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.	• Dashboard or any other integration of the IR plan throughout the organization • Automation of updating the IR plan • Evidence of DHS's Cyber Storm exercise participation

Assessor Best Practices
Defined: The assessor should ensure the IR Plan includes the defined requirements listed above in the Defined section. **Consistently Implemented:** A few examples of incidents and how it was detected, analyzed, handled, and reported would also help support the consistently implemented maturity level for other metrics in this domain such as 53, 54, 55, and 56. **Managed and measurable:** Metrics should be defined in the IR Plan. The agency could demo or the assessor could observe how the metrics are collected, who they are reported to, and how they are used to update the IR Plan. **Optimized:** Integration with other agency offices, such as exercises.

53. To what extent have incident response team ***structures/models, stakeholders, and their roles, responsibilities***, levels of authority, and dependencies been defined, communicated, and implemented across the organization?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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 • US-CERT Federal Incident Notification Guidelines • Green Book: Principles 3, 4, and 5	FY2024	**Ad Hoc** Roles and responsibilities have not been fully defined and communicated across the organization, including appropriate levels of authority and dependencies.	
		Defined 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 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.	• IR Plan • IR policies and procedures • Security Operations Center demo
		Consistently Implemented Individuals are performing the roles and responsibilities that have been defined across the organization.	• Incident response tickets • Email or other communications of responsible stakeholders.
		Managed and Measurable Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement incident response activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	• Responsible, Accountable, Consulted, and Informed (RACI) chart.
		Optimized The organization continuously evaluates and adapts its incident response-based roles and responsibilities to account for a changing cybersecurity landscape.	• Updates to IR plans, policies, procedures, playbooks, guidance.

Assessor Best Practices
Defined: **Consistently Implemented:** Examples of incident response tickets could be used to assess other metrics in this domain such as 52, 54, 55, and 56. **Managed and measurable:** **Optimized:**

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

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53 (Rev. 5): IR-4, IR-5, and IR-6 • NIST SP 800-61 (Rev. 2) • NIST SP 800-92 • NIST CSF: DE.AE-1 -5, PR.DS-6, RS.AN-1, RS.AN-4, and PR.DS-8 • EO 14028: Section 6 • OMB M-20-04 • OMB M-21-31 • OMB M-22-01 • OMB M-24-04 • CISA Cybersecurity Incident Response Playbooks • CIS Top 18 Security Controls: Control 17	Core	**Ad Hoc** 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.	
		Defined 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.	• Incident detection and analysis strategies, policies, procedures, and standards, including a common threat vector taxonomy • Enterprise-level incident response plan • Network architecture diagram highlighting the layers of protection/technologies in place to detect and analyze incidents. • SOPs for supporting technologies used to detect/analyze potential incidents.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• US-CERT Federal Incident Notification Guidelines • CISA Guidance for Implementation of M-21-31		**Consistently Implemented** 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.	• Sample of incident tickets, including those submitted to US-CERT. • Evidence of configurations that show the precursors and indicators captured for the tools listed in Question #58 and for the following tools: • Web application protections, such as web application firewalls. • Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools. • Aggregation and analysis, such as security information and event management (SIEM) products. • Malware detection, such as antivirus and antispam software technologies. • Information management, such as data loss prevention • File integrity and endpoint and server security tools. • Evidence of capturing lessons learned on the effectiveness of the incident detection and analysis policies and procedures. • Endpoint Detection and Response (EDR). • Working w/CISA to identify implementation gaps, coordinate deployment of EDR tools. • Ensuring EDR tools meet CISA requirements.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable 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.	• Baseline of expected data flows and network operations. • Evidence of checksums for critical files. • Evidence of use of performance metrics defined in the incident detection and analysis policies, procedures, and plan.
		Optimized The organization is making demonstrated progress towards implementing EL3's (advanced) requirements for its logging capabilities.	

Assessor Best Practices
Defined: Assessors should ensure the agency's logging policies, procedures, and processes prioritizes high value asset (HVA) systems, high impact systems, and the enterprise IT network (including cloud service providers) to meet the requirements of M-21-31. Assessors should evaluate how the agency has made risk-informed decisions about where log collection is most beneficial for improving cybersecurity incident detection and investigation and that this is captured in the organization's policies, procedures, and processes. **Consistently Implemented:** Observe technologies and tools supporting incident detection and analysis to verify whether the defined indicators and precursors are being captured and reviewed. As of August 2022, agencies are required to meet the EL1 logging level as directed by M21-31. Assessors evaluate the implemented logging processes and procedures against the EL1 logging requirements of M-21-31 and CISA implementation guidance. Agencies must collect all Criticality 0 log types to be EL1 compliant. IGs can assess agency actions to implement integrity measures limiting access to and allowing cryptographic verification of logs, as well as logging DNS requests made throughout their environment. **Managed and measurable:** As of February 2023, agencies are required to meet the EL2 logging level as directed by M21-31. Evaluate the implemented logging processes and procedures against the EL2 logging requirements of M-21-31 and CISA implementation guidance. **Optimized:** As of August 2023, agencies are required to meet the EL3 logging level as directed by M21-31. Evaluate the implemented logging processes and procedures against the EL3 logging requirements of M-21-31 and CISA implementation guidance.

55. How mature are the organization's ***processes for incident handling***?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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	Core	**Ad Hoc** 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.	

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• EO 14028: Section 6 • OMB M-21-31 • OMB M-24-04 • CISA Cybersecurity Incident Response Playbooks		**Defined** 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.	• Containment strategies for each major incident type. • Incident response policies, procedures, and plans.
		Consistently Implemented 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.	• Sample of incident tickets to obtain evidence that incident handling policies and procedures, containment strategies, and incident eradication processes were followed. • Evidence that vulnerabilities that were exploited and resulted in incidents were remediated (e.g., vulnerability scanning reports, or additional training) • Evidence of capturing lessons learned on the incident handling policies and procedures.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable 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.	• Evidence of use of performance metrics for containment and eradication defined in the incident response policies, procedures, and plan. • Evidence of verifications / validation of data feeding the metrics. • Metrics related to successful incidents that measure impact and timeliness of vulnerability mitigation on other systems.
		Optimized 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.	• Observe technologies in use for dynamic reconfiguration of network devices in response to incident types.

Assessor Best Practices
Defined: **Consistently Implemented:** **Managed and measurable:** **Optimized:**

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?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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	FY2024	**Ad Hoc** 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.	
		Defined 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.	• IR Plan • IR policies and procedures • Reporting processes • Email or other communication of how to report incidents
		Consistently Implemented 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.	• Examples of incident response tickets • Evidence of reporting to US-CERT • Evidence of reporting to law enforcement • Evidence of reporting to OIG • Evidence in reporting to Congress.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable 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.	• Metrics defined in the IR Plan • Evidence of how this data is captured
		Optimized The organization receives, retains, uses, and disseminates cyber threat indicators in accordance with the Cybersecurity Information Sharing Act of 2015.	• Documented cyber threat indicators

Assessor Best Practices
Defined: Ensure the IR documentation includes how to report security incident information, including for major incidents, to US-CERT, law enforcement, the Congress and the Office of Inspector General, as appropriate. **Consistently Implemented:** If the evidence is available. In some cases, no major incidents may have occurred over the past fiscal year. If no major incidents, ensure the incident response information is shared with individuals with responsibilities within the agency. Ensure the information sharing is done within agency and Federal guidelines. **Managed and measurable:** The evidence of the metrics can be used to assess other metrics in this domain such as 52, 53, 54, and 55. **Optimized:** Follow the guidance in the Cybersecurity Information Sharing Act of 2015.

57. To what extent does the ***organization collaborate with stakeholders*** to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53 (Rev. 5): IR-4 • NIST SP 800-86 • OMB M-20-04 • PPD-41 • NCPS Cloud Interface Reference Architecture	FY2023	**Ad Hoc** The organization has not defined how it will collaborate with DHS and other parties, as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. In addition, the organization has not defined how it plans to use DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks.	
		Defined The organization has defined how it will collaborate with DHS and other parties, as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. This includes identification of incident response services that may need to be procured to support organizational processes. In addition, the organization has defined how it plans to use DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks.	• Contracts/Task Orders/SOWs/service level agreements for incident response services. • MOAs/MOUs with DHS. • DHS Einstein program plan utilization.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented The organization consistently uses on-site, technical assistance/surge capabilities offered by DHS or ensures that such capabilities are in place and can be leveraged when needed. In addition, the organization has entered contractual relationships in support of incident response processes (e.g., for forensic support), as needed. The organization has fully deployed DHS' Einstein 1 and 2 to screen all traffic entering and leaving its network through a TIC.	• Evidence of monitoring feeds from DHS related to Einstein 1 and 2. • Evaluate the agency's timeliness of requested incident response services and assess the agency's quality of the services being provided.
		Managed and Measurable The organization uses Einstein 3 Accelerated, and/or other comparable tools or services, to detect and proactively block cyber-attacks or prevent potential compromises.	• Evidence of monitoring feeds from DHS related to Einstein 3A.
		Optimized The organization is making progress in implementing information sharing and reporting patterns to provide telemetry information to CISA for its cloud-based environments not covered by Einstein 3 Accelerated.	• Reporting patterns provided to CISA for cloud-based environments.

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized:

58. To what extent does the organization utilize the following ***technology to support its incident response*** program?

- Web application protections, such as web application firewalls
- Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools
- Aggregation and analysis, such as security information and event management (SIEM) products
- Malware detection, such as antivirus and antispam software technologies
- Information management, such as data loss prevention
- File integrity and endpoint and server security tools

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-44 • NIST SP 800-61 (Rev. 2) • NIST SP 800-137 • OMB M-22-01 • OMB M-22-09	FY2023	**Ad Hoc** The organization has not identified and defined its requirements for incident response technologies needed in one or more of the specified areas and relies on manual/procedural methods in instances where automation would be more effective.	
		Defined The organization has identified and fully defined its requirements for the incident response technologies it plans to use in the specified areas. While tools are implemented to support some incident response activities, the tools are not interoperable to the extent practicable, do not cover all components of the organization's network, and/or have not been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, plans, and procedures.	• Incident response plan and strategies, including defined requirements for the incident response program. • SOPs for the tools being used. • Network architecture diagram.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented The organization has consistently implemented its defined incident response technologies in the specified areas. In addition, the technologies used are interoperable to the extent practicable, cover all components of the organization's network, and have been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, procedures, and plans.	• List of feeds into the agency's SIEM tool. • Walkthrough and capture screenshots of the technologies being used to verify coverage of the organization's network and the extent to which they are interoperable. Further, walkthrough whether the tools can identify the source and the target(s) of the information being flagged.
		Managed and Measurable The organization evaluates the effectiveness of its incident response technologies and makes adjustments to configurations and toolsets, as appropriate.	• Evidence of use of performance metrics/dashboards defined in the incident response policies, procedures, and plan. • Evidence of verifications/validation of data feeding the metrics/dashboards.
		Optimized The organization has institutionalized the implementation of advanced incident response technologies for analysis of trends and performance against benchmarks (e.g., simulation-based technologies to continuously determine the impact of potential security incidents to its IT assets) and adjusts incident response processes and security measures accordingly.	• Results of trend analysis, benchmarking, and the resulting updates made to the incident response program. • Evidence of use of simulation technologies to model the impact of an incident on the agency's environment.

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized:

59. Provide any additional information on the effectiveness (positive or negative) of the organization's ***incident response program*** that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the incident response program effective?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
	Annual	**Ad Hoc**	•
		Defined	•
		Consistently Implemented	•
		Managed and Measurable	•
		Optimized	•

Assessor Best Practices

Defined:

Consistently Implemented:

Managed and measurable:

Optimized:

Contingency Planning (CP)

60. To what extent have ***roles and responsibilities*** of stakeholders involved in information systems contingency planning been defined, communicated, and implemented across the organization, including appropriate delegations of authority?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-34 • NIST SP 800-53 (Rev. 5): CP-1, CP-2, and CP-3 • NIST SP 800-84 • FCD-1: Annex B	FY2023	**Ad Hoc** Roles and responsibilities have not been fully defined and communicated across the organization, including appropriate delegations of authority.	
		Defined Roles and responsibilities of stakeholders have been fully defined and communicated across the organization, including appropriate delegations of authority. In addition, the organization has designated appropriate teams to implement its contingency planning strategies. Further, the organization has defined its policies and procedures for providing contingency training consistent with roles and responsibilities.	• Information security strategy and policy. • Information system contingency planning strategy, policies, and procedures. • Agency-wide continuity of operations, business continuity, or disaster recovery plans, policies, and procedures. • Review delegations of authority and organizational charts. • Evidence policies and procedures define role-based contingency plan training.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented Individuals are performing the roles and responsibilities that have been defined across the organization. The organization ensures that contingency training is provided consistent with roles and responsibilities to ensure that the appropriate content and level of detail is included.	• Interview individuals involved in the contingency planning and recovery process to confirm their roles and responsibilities. • Current organization chart showing whether defined roles are filled. • Review a sample of continuity of operations, business continuity, or disaster recovery plan exercises. • Review Plan of Action and Milestones for identified weaknesses in contingency planning that could indicate problems related to roles and responsibilities. • Sample after-action reports for contingency exercises for lessons learned.
		Managed and Measurable Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement system contingency planning activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	• Review sample of Information system contingency plans to ensure that resources and timeframes are assigned using a risk-based approach. • Review contingency plan test results to determine if contingency plan activities were successful with established resources; determine if lessons learned mentions resource needs. • Established qualitative or quantitative metrics to ensure the effectiveness of the contingency planning and hold stakeholders accountable for their roles and responsibilities.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Optimized The organization incorporates simulated events into contingency training to facilitate effective response by stakeholders (internal and external) involved in information systems contingency planning and to measure the extent to which individuals are equipped to perform their roles and responsibilities.	• Evidence that demonstrates that the organization incorporates simulated events into its contingency planning exercises. • Established qualitative or quantitative metrics to ensure the effectiveness of the contingency planning and using that information to make continuous improvements.

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized:

61. To what extent does the organization ensure that the results of ***business impact analyses (BIA)*** are used to guide contingency planning efforts?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-34, Rev. 1, 3.2 • NIST SP 800-53, Rev. 5: CP-2, and RA-9 • NIST IR 8179	Core	**Ad Hoc** 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.	

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST IR 8286 • NIST IR 8286D • NIST CSF: ID.RA-4 • FIPS 199 • FCD-1 • FCD-2 • OMB M-19-03		**Defined** 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.	• Information security strategy and policy. • Information system contingency planning strategy, policies, and procedures, including the requirements to use Business Impact. • Business Impact Analysis policies, procedures, and processes.
		Consistently Implemented 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, and 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.	• Templates for completing BIAs. • Review organizational level BIAs to ensure it includes system-level components, missions, and recovery critically/priorities into strategy and plan development. • Sample system-level BIAs or information system contingency plans to ensure that BIAs are used to determine contingency planning requirements and priorities, including mission essential functions/high value assets. • Recent CIO Metric 10.1.4 results to ensure organizational systems are covered by business impact analysis.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable 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 utilizes the results of its BIA in conjunction with its risk register to calculate potential losses and inform senior level decision making.	• Evidence that BIA results are integrated with organizational ERM processes. • Review meeting minutes supporting that the enterprise risk management processes include BIAs as part of the evaluating and monitoring of the criticality and sensitivity of enterprise assets. • Evidence that BIA results are integrated with the organization's risk register to calculate potential losses and inform decision making
		Optimized 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.	• Evidence that the organization uses BIA results in conjunction with its risk register to improve risk identification and response. • Evidence that the organization's planning efforts reduced its risk profile and facilitated effective risk responses

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized:

62. To what extent does the organization ensure that information system ***contingency plans are developed, maintained, and integrated*** with other continuity plans?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-34 • NIST SP 800-53 (Rev. 5) CP-2 • NIST CSF: PR.IP-9 • FY 2024 CIO FISMA Metrics: 10.1, 10.2, and 10.3 • OMB M-19-03	FY2024	**Ad Hoc** 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.	
		Defined 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 plan policies, procedures, guidance documents, etc. • Enterprise wide information system security policies.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented 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 business process continuity, disaster recovery planning, incident management, insider threat implementation plan (as appropriate), and occupant emergency plans.	• For a sample of systems, inspect and analyze system-specific contingency plans. • Analyze other continuity documents/requirements to ensure integration (i.e. Disaster Recovery Plan, Continuity of Operations Plan, Business Continuity Plan, Incident Response Plans, emergency plans, Business Impact Analysis documents, etc.) • Ensure contingency planning is integrated into the Cybersecurity Framework scorecard.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable 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. The organization coordinates the development of ISCP's with the contingency plans of external service providers.	• Evidence of performance metrics and/or dashboards used that deliver persistent situational awareness across the organization. • Evidence of tacking in scorecard or forums. • For cloud systems/vendors, inspect evidence detailing how the organization ensures development of ISCP's with the contingency plans of the external service providers. • Testing of plans either through tabletop exercises or disaster recovery testing. • After Action Reports are documented and maintained and used to update current planning documents. • Corrective action plans from audits and reviews are developed, documented, and implemented. • Ensure contingency planning is integrated into the ongoing security authorization process.
		Optimized 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.	• Obtain evidence on how the results of the enterprise/system contingency planning program are integrated into to the agency's enterprise risk management program, strategic planning processes, capital allocation/budgeting, and other mission/business areas on a near-real time basis.

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized:

63. To what extent does the organization perform tests/exercises of its information system contingency planning processes?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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 v.8: Control 11	Core	**Ad Hoc** 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.	
		Defined 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 security strategy and policy. • Information system contingency planning strategy, policies, and procedures, including the requirements to perform tests or exercises.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented 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.	• Sample information system contingency planning testing results. • Results of testing of continuity of operations, business continuity, or disaster recovery plans. • Review the independent assessment of CP-4 security control across the organization. Assessment determines whether contingency plans are tested, test results are reviewed, and corrective action are in-place if needed. • Evidence of after-action reports and that officials used the result to improve the contingency planning efforts.
		Managed and Measurable 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.	• Review the results of information system contingency plan testing and exercises for selected systems. • Review the independent assessment of CP-4(3) security control across the organization. Assessment determines whether contingency plan is tested using automated mechanisms. • Coordination emails and test/exercise plans. • Review after action review results to verify external stakeholder activity.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Optimized 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.	• Evidence of organization defined mechanisms to disrupt or adversely affect the system or system components on a risk basis that demonstrates the effectiveness of testing and the contingency planning process, including full system recovery. • Review the independent assessment of CP-4(4) and CP-4(5). Assessment of CP-4(4) determines whether system has been fully recovered and reconstituted as a part of testing. CP-4(5) determines how resilient a system is using self-inflicted system disruptions (e.g., terminating system components) to reveal unknown component/service dependencies.

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized:

64. To what extent does the organization perform ***information system backup and storage***, including use of alternate storage and processing sites, as appropriate?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• 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 2024 CIO FISMA Metrics: 10.3.1 and 10.3.2 • NIST Security Measures for EO- Critical Software Use: SM 2.5	FY2024	**Ad Hoc** 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.	
		Defined 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.	• Information system contingency planning policies, procedures, guidance documents, etc. • Enterprise wide information system security policies. • Determine if supply chain alternatives are incorporated into its contingency planning strategy.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Consistently Implemented 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 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.	• For a sample of systems, inspect and analyze system-specific contingency plans and system security plans. • Analyze other continuity documents/requirements to ensure integration (i.e. evidence of user- and system-level backups for a defined timeframe) • For a sample of systems, evidence of risk assessment being performed to ensure the proper selection of alternative storage and processing sites. • Determine if alternate testing sites are included in disaster recovery testing and if so, are these sites included in annual testing.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable 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.	• Evidence of independent assessment/monitoring reports of the chosen facilities/sites. • Dashboard/metrics are used and analyzed as part of the continuous monitoring process to ensure proper configuration. • Ensure backup and storage are integrated into the ongoing security authorization.
		Optimized 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.	• Inspect and analyze system security plans, incident response plans, and information security contingency plans to ensure appropriate controls and steps in place to protect against infection or other compromise of its backup data. • Analyze a sample of security incidents relating to alternative storage and processing sites to determine if the incident response plans were followed correctly. • Screenshots/automated alerts showing periodical scans of past backups with current anti- malware tools to identify poisoned backups.

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized:

65. To what level does the organization ensure that information on the planning and performance of ***recovery activities is communicated*** to internal stakeholders and executive management teams and used to make risk-based decisions?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53 (Rev. 5): CP-2 and IR-4 • NIST CSF: RC.CO-3	FY2023	**Ad Hoc** The organization has not defined how the planning and performance of recovery activities are communicated to internal stakeholders and executive management teams and used to make risk-based decisions.	
		Defined The organization has defined how the planning and performance of recovery activities are communicated to internal stakeholders and executive management teams.	• Information security strategy and policy. • Information system contingency planning policies and procedures. • Information system contingency plan testing schedule.
		Consistently Implemented Information on the planning and performance of recovery activities is consistently communicated to relevant stakeholders and executive management teams, who use the information to make risk-based decisions.	• Evidence of communication of recovery activities (e.g., after-action reports, POA&Ms, etc.) to contingency planning stakeholders for coordinated testing/activities. • Evidence showing that items within after-action reports are remediated.

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
		Managed and Measurable Metrics on the effectiveness of recovery activities are communicated to relevant stakeholders and the organization has ensured that the data supporting the metrics are obtained accurately, consistently, and in a reproducible format.	• Established qualitative or quantitative metrics/dashboards to ensure the effectiveness of the contingency planning. • Evidence of use of performance metrics/dashboards. • Evidence of verification and validation of data feeding the metrics/dashboard.
		Optimized The organization ensures that information on the planning and performance of recovery activities for its ICT supply chain providers is integrated into its communication processes on a near real-time basis.	• Evidence that information from organizational contingency planning efforts is integrated with supply chain risk planning that can adjust to emerging (evolving) or near real-time threats. • Evidence of documented communication channels with ICT (information and communications technology) providers.

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized:

66. Provide any additional information on the effectiveness (positive or negative) of the organization's ***contingency planning program*** that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the contingency planning program effective?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
	Annual	**Ad Hoc**	•
		Defined	•
		Consistently Implemented	•
		Managed and Measurable	•
		Optimized	•

Assessor Best Practices
Defined:
Consistently Implemented:
Managed and measurable:
Optimized: