FY 2025
Inspector General
Federal Information
Security Modernization Act of 2014
(FISMA) Metrics
Evaluator's Guide

VERSION 1.0

MAY 5, 2025

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 2025 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 and red team assessment 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 2025 IG FISMA metrics[1] and OMB M-25-04[2] which 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.[3] If an agency does not reach level 4 or above for any metric, IGs are required to provide a summary in DHS's CyberScope portal as to why that metric only achieved level 3 or below. This provides the agency with adequate justification for not reaching an effective level of security. IG should write level 4 and its gaps in maturity. For example, "The Agency

[1] Final FY 2025 IG FISMA Reporting Metrics (cisa.gov)
[2] Office of Management and Budget Memorandum M-25-04
[3] NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations

information security program is not effective because …." 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 (i.e. govern, 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 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, 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. To facilitate this shift, and provide a foundation for assessing risk-based security objectives, starting in FY 2025, IGs are required to assess the extent to which agencies develop and maintain cybersecurity profiles that are used to understand, tailor, assess, prioritize and communicate cybersecurity objectives.

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 not considered a core metric but represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness. For FY 2025, the supplemental metrics comprise of five new metrics designed to gauge the maturity of agencies' cybersecurity governance practices and implementation of key components of ZTA. These five metrics will be evaluated by IGs and scored in FY 2025. IG wills consider the supplemental metric ratings when making the domain and function level maturity determinations.

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.[4]

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.

The term "*information system*", "*FISMA system*", and "*system*" are often used interchangeably. For the purposes of FISMA and this document, an "*information system*" is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. According to FISMA, the head of Federal agencies are responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems used or operated by their agency or on behalf of their agency by a contractor or other organization.

Alternative Evidence Considerations

While the tables below provide recommended types of evidence for evaluating maturity levels, IGs should consider accepting additional forms of evidence that effectively demonstrate capability maturity. The following alternative evidence approaches could complement traditional documentation:

1. Demonstrated Capability: Direct observation or demonstration of security capabilities functioning in actual operational environments.
2. Results-oriented: Data showing measurable improvements in security posture (e.g., reduction in incidents, faster response times).
3. Performance Testing: Results and actions taken to address findings from penetration tests, tabletop exercises, or security simulations.
4. Continuous Monitoring Data: Metrics and alerts from active monitoring systems.
5. Adaptability: Examples of how the agency has adjusted controls in response to emerging threats.
6. Integration: Demonstration of how controls work together as a cohesive system rather than isolated components.

These alternative forms of evidence may be particularly valuable when traditional documentation does not fully capture the effectiveness of an agency's security program. The intent of these suggestions is to support a holistic assessment approach that values security effectiveness alongside formal documentation.

[4] NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Management

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.

How should a recommendation be written?
To facilitate a steady progression through the maturity model,[5] 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.

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

[5] FY 2025 Inspector General FISMA Reporting Metrics, pg. 8

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 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.

How should IGs handle challenges in performing FISMA evaluations that may arise, for example, from reorganizations and personnel changes?

Consistent with Government Auditing Standards (Yellow Book) and CIGIE's Quality Standards for Inspection and Evaluation (Blue Book), IGs should document the impact that scope limitations, restrictions on access to records, or other issues affecting their ability to complete FISMA reviews. Further, IGs should explain in CyberScope the impact this has on the IGs ability to determine the effectiveness of their agency's information security program.

The tables below show the IG metrics for FY25 IG evaluation period.

Cybersecurity Governance			
1. To what extent does the organization develop and maintain cybersecurity profiles that are used to understand, tailor, assess, prioritize and communicate its cybersecurity objectives?			
Criteria	**Review Cycle**	**Maturity Level**	**Suggested Standard Source Evidence**
• OMB Circular A-123 • OMB Circular A-130 • FISMA 2014 **Supplemental Guidance:** • NIST CSF v2.0: Section 3.1 • NIST CSF v2.0: GV.0C-01 • NIST CSF v2.0: GV.OC-02 • NIST CSF v2.0: GV.OC-03 • NIST CSF v2.0: GV.OC-04 • NIST CSF v2.0: GV.OC-05 • NIST CSF v2.0: GV.OV-01 • NIST CSF v2.0: GV.OV-02	FY 2025 Supplemental	**Ad Hoc** The organization has not defined a formal process for developing and maintaining current and target cybersecurity profile(s).	
		Defined The organization has defined policies and procedures for developing and maintaining current and target profile(s) that includes, at a minimum, consideration of the organization's mission objectives, threat landscape, resources (including personnel), and constraints. The organization has determined the scope of its profile(s) (e.g. Entity level, division level, process level, system level).	• Cybersecurity program policy; • Cybersecurity Risk Management policies, procedures, strategies; • Cybersecurity Framework profiles; • Information Security Program Plan; • Privacy Risk Assessments.
		Consistently Implemented. The organization develops and maintains current and target cybersecurity profile(s).	• Risk management policies, procedures, and strategies, lessons learned; • Enterprise Risk Profiles; • Cybersecurity Framework profiles;

• NIST CSF v2.0: GV.OV-03 • NIST SP 800-53, Rev. 5, PM-1, PM-11		The target profile(s) considers anticipated changes to the organization's cybersecurity posture. The organization assesses the gaps between its current and target profiles and creates and implements a prioritized action plan.	• Current and target cybersecurity profile strategies, plans, and other documents; • Cybersecurity Framework current/future state implementation documentation.
		Managed and Measurable The organization periodically monitors and reports on progress in reaching its target profiles through measurable objectives. Cybersecurity profiles align with the organization's risk strategy and are used to align security architectures and investments. The organization refines its organizational profiles periodically based on known risk exposure and residual risk.	• Cybersecurity Framework profiles, periodic reviews of risk tolerance levels, etc.; • Cybersecurity Framework future state implementation documentation; • Governance, Risk, and Compliance (GRC) dashboards/reports; • CSRR(s); • Continuous monitoring dashboards and reports (e.g., CDM and SIEM outputs/alerts/reports, vulnerability management dashboards, etc.).
		Optimized The organization continuously monitors (i.e. near real-time) the achievement of cybersecurity risk management objectives, leveraging predictive analytics and threat intelligence to adjust its target profiles, when necessary.	• Cybersecurity Framework profiles, continuous reviews of risk tolerance levels, etc.; • Enterprise risk profiles; • Enterprise-wide and component-level risk management dashboards;

		As applicable, the organization uses its current profile to document and communicate the organization's cyber capabilities with external stakeholders. As applicable, the organization uses its target profile to express the organization's cyber risk management requirements and expectations with external stakeholders.	• Current and Target-state cyber risk profile (see NIST CSF, section 3.3); • Organization-wide risk assessments/risk registers; • Organization-wide risk dashboards; • Cyber risk dashboards; • Enterprise risk management program artifacts.

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

2. To what extent does the organization use a cybersecurity risk management strategy to support operational risk decisions?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• OMB Circular A-123 • OMB Circular A-130 • FISMA 2014 **Supplemental Guidance:** • NIST CSF v2.0: GV.RM-01 • NIST CSF v2.0: GV.RM-02 • NIST CSF v2.0: GV.RM-03 • NIST CSF v2.0: GV.RM-04	FY 2025 Supplemental	**Ad-Hoc** The organization has not developed a risk management strategy that defines the organization's priorities, constraints, risk tolerance and appetite statements, and assumptions.	
		Defined The organization has developed a risk management strategy that includes the organization's priorities, constraints, risk tolerance and appetite statements, and assumptions.	• Enterprise Risk Management policies, procedures, and strategies; • Cybersecurity Risk Management policies, procedures, strategies;

• NIST CSF v2.0: GV.RM-06 • NIST SP 800-53 Rev. 5: PM-9, PM-28, and RA-7		Risk management objectives have been established and agreed to by organizational stakeholders. Lines of communication are established for cybersecurity risks, including risks from suppliers and other third-parties.	• Risk Assessment Policies and Procedures; • Ongoing Authorization policies and procedures; • Organizational risk profiles; • SDLC policies and procedures; • EA policies and procedures; • Risk Executive Council Charters/delegations of authority.
		Consistently Implemented The organization consistently implements its risk management strategy at the organizational, mission/business process, and system levels. The organization consistently evaluates and adjusts its cybersecurity risk management strategy based on its threat environment and organization wide cyber and privacy risk assessment. The organization consistently calculates, documents, categorizes and prioritizes cybersecurity risks.	• Risk Executive Council Charters; • Risk Council meeting minutes; • Organizational, Mission, and System-level Risk Assessments; • System Security Plans; • Security Assessment Reports; • System Risk Assessments; • Privacy Threshold Analysis (PTA); • Privacy Impact Assessment (PIA);

			• 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.
		Managed and Measurable The organization uses qualitative and quantitative data to assess cybersecurity risk management effectiveness. Metrics, dashboards, and automated tools inform adjustments to the strategy.	• Organization-wide risk assessment(s); • CSRR(s)s; • Risk Executive Council Charters;

		The organization's cyber risk management strategy integrates security and privacy programs with the management control systems established in the organization's enterprise risk management strategy.	• Risk Council meeting minutes; • System-level risk assessments; • Privacy risk assessments; • 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.

		Optimized The organization continuously monitors its cybersecurity risk management program in near real-time, leveraging predictive analytics and threat intelligence to proactively adjust strategies. Governance structures ensure near real-time decision-making. 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.	• 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: **Consistently Implemented:** **Managed and measurable:** **Optimized:**

3. To what extent do cybersecurity roles, responsibilities, and authorities foster accountability, performance assessment, and continuous improvement?			
Criteria	**Review Cycle**	**Maturity Level**	**Suggested Standard Source Evidence**
• OMB Circular A-123 • OMB Circular A-130 • FISMA 2014 **Supplemental Guidance** • NIST FIPS 200 • 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 • NIST CSF v2.0: GV.RR-01	FY 2025 Supplemental	**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 team, roles and responsibilities of stakeholders, and levels of authority and dependencies.	• Information security program policy; • Organizational 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 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;

• NIST CSF v2.0: GV.RR-02 • NIST CSF v2.0: GV.RR-03 • NIST CSF v2.0: GV.RR-04 • NIST SP 800-53 Rev. 5: PM-2, PM-3, PM-13, PM-23, PM-29, PS-9		**Managed and Measurable** Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement cybersecurity activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	• Evidence of use of performance metrics/dashboards defined in the organizational strategy; • Evidence of verifications/validation of data feeding the metrics/dashboard; • Evidence of coordination amongst other related security domains; • Evidence that individuals with security responsibilities are held accountable (e.g., performance rating templates or similar documentation).
		Optimized: The organization continuously evaluates and adapts its cybersecurity roles and responsibilities to account for a changing cybersecurity landscape.	• Evidence of input/knowledge/guidance/lessons learned from oversight agencies (DHS, OMB, CISA, etc.) are being incorporated into decision making for resource allocation.

Assessor Best Practices
Defined: Review the security plan and ensure the organization has defined roles and responsibilities. **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 adequate resources. **Managed and measurable:** Assessor should evaluate whether the organization has defined metrics to assess 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 decision making.

4. Provide any additional information on the effectiveness (positive or negative) of the organization's cybersecurity governance 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 cybersecurity governance 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:**			

Cybersecurity Supply Chain Risk Management (C-SCRM)			
5. 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**
• OMB A-130 • OMB M-19-03 • OMB M-22-18 • The Federal Acquisition Supply Chain Security Act of 2018 • EO 14028 **Supplemental Guidance** • NIST SP 800-53 (Rev. 5): SA-4, SR-3, SR-5, and SR-6 • NIST SP 800-152 • NIST SP 800-161 (Rev. 1) • NIST SP 800-218: Task PO.1.3 • NIST IR 8276	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.	
		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 C-SCRM measures for external providers.	• 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.

• NIST CSF: GV.SC • CIS Top 18 Security Controls: Control 15 • FedRAMP standard contract clauses • Cloud computing contract best practices • DHS's ICT Supply Chain Library • NIST CSF v2.0: GV.SC-01 through GV.SC-07		• Tools and techniques to use the acquisition process to protect the supply chain, including, risk-based processes for evaluating cyber supply chain risks associated with third party providers, as appropriate. Contract tools or procurement methods to confirm contractors are meeting their contractual C SCRM obligations.	
		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.	• 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, such as cybersecurity, IT, operations, legal, HR and Engineering teams; • Log showing lessons learned used to update the SCRM strategy; • Evidence of communication regarding issues and challenges in reducing the risk

		Furthermore, the organization maintains visibility into its upstream suppliers and can consistently track changes in suppliers	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.
		Managed and Measurable The organization uses qualitative and quantitative performance metrics (e.g., those defined within SLAs) to measure, report on, and monitor the C-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 cyber-related supply chain risks	• 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.
		Optimized The organization analyzes, in a near-real time basis, the impact of material changes to C-SCRM assurance requirements on its relationships with external providers and ensures that acquisition tools, methods, and processes are updated as soon as possible	• 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:

6. 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 supply chain risk management 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:**

Risk and Asset Management (RAM)			
7. 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**
• FISMA 2014 • Federal Information Technology Acquisition Reform Act (FITARA) of 2014 • OMB M-16-12 • OMB M-19-03 • OMB M-21-31 • OMB Circular A-130 • OMB Circular A-123 • OMB M-25-04 • NIST FIPS 200 • NIST FIPS 199	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;

Supplemental Guidance • NIST CSF v2.0: ID.AM-01 • NIST CSF v2.0: ID.AM-02 • NIST CSF v2.0: ID.AM-03 • NIST CSF v2.0: ID.AM-04 • NIST SP 800-53 (Rev. 5): CA-3, PM-5, and CM-8 • NIST SP 800-37 (Rev. 2) • FY 2025 CIO FISMA Metrics: 1.1 and 1.5 • OMB M-21-31, CISA Operational Guidance			• Ongoing authorization policies and procedures.
		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; • Change control requests; • FedRAMP PMO communications; • EA Documentation; • Web app domain registry information.
		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 Information Security Continuous Monitoring (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	• Dashboard reports/observations; • Hardware and software component inventories;

		organizational information systems. The centralized inventory is updated in a near-real time basis.	• Asset database reports; • Evidence the reports and alerts which indicate changes to the inventory are updated in real-time.

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 respond 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.

8. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including Government Furnished Equipment (GFE), Internet of Things [IoT], 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
• FISMA 2014 • FITARA 2014 • OMB M-25-04 • OMB Circular A-130 • OMB Circular A-123 • DHS Binding Operational	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 (including through automated asset discovery) with the detailed information necessary for tracking and reporting	

Directive (BOD) 23-01 • DHS BOD 23-02 **Supplemental Guidance** • NIST CSF v2.0: ID.AM-01 • NIST SP 800-53 (Rev. 5): CA-7 and CM-8 • NIST 1800-5 • NIST IR 8011 • 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		**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.
		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	• 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);

• CIS Top 18 Security Controls: Control 1 • BOD 23-01 Implementation Guidance • NIST SP 800-37 (Rev. 2): Tasks P-10 and P-16 • FY 2025 CIO FISMA Metrics: 1.2, 1.3, and 10.8		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' Continuous Diagnostics and Mitigation (CDM) program	• 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).
		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, SOAR, SIEM, 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	• ITAM/hardware asset management reports; • Mobile Device Management solution configuration or reports; • Continuous monitoring dashboards or reports;

		organization's enterprise architecture current and future states.	• 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.

9. 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**
• FISMA 2014 • FITARA 2014 • OMB M-25-04 • OMB Circular A-130 • OMB M-21-30 • EO 14028 • OMB M-22-18 **Supplemental Guidance** • NIST CSF v2.0: ID.AM-02 • NIST SP 800-53 (Rev. 5): CA-7, CM-8, CM-10, and CM-11 • NIST SP 800-37 (Rev. 2): Task P-10 • NIST SP 800-137 • NIST SP 800-207: Section 7.3 • NIST 1800-5 • NIST IR 8011 Vol. 1 • NIST IR 8011 Vol. 3 • NIST Security Measures for EO-Critical Software Use	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.	
		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;

• FY 2025 CIO FISMA Metrics: 1.4 and 4.1-4.4 • OMB M-21-30 • OMB M-22-18 • OMB M-25-04 • FISMA 2014 • FITARA 2014 • OMB Circular A-130 • EO 14028 • CIS Top 18 Security Controls: Control 2 • CISA Cybersecurity Incident Response Playbooks			• 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.
		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.).
		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, SOAR, 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.

10. To what extent does the organization develop and maintain inventories of data and corresponding metadata for designated data types, as appropriate throughout the data lifecycle?			
Criteria	**Review Cycle**	**Maturity Level**	**Suggested Standard Source Evidence**
• FISMA 2014 • Privacy Act of 1974 • Federal Records Act • 44 U.S. Code Section 3511 – Data Inventory and Federal Data Catalogue • EO 14028 **Supplemental Guidance** • NIST SP 800-171 Rev. 3 • CIS Critical Security Controls: 3.2 • Federal Zero Trust Data Security Guide • NIST CSF v2.0: ID.AM-07 • NIST SP 800-53 Rev. 5: AC-4, CM-12, CM-13, and RA-2	FY 2025 Supplemental	**Ad Hoc** The organization has not defined its policies, procedures, processes, and roles and responsibilities for developing and maintaining a comprehensive and accurate inventory of data and corresponding metadata for its data types, as appropriate. This includes data obtained from third party providers.	
		Defined The organization has defined its policies, procedures, processes, and roles and responsibilities for developing and maintaining a comprehensive and accurate inventory data and corresponding metadata for its data types, to include data obtained from third party providers, as appropriate	• Data classification policy, including the identification of agency specific data that could include PII, PHI, financial account numbers, intellectual property, operational technology data, etc.; • Data Dictionary/Metadata Repository; • Data Lifecycle Management Policy.
		Consistently Implemented The organization consistently implements its policies, procedures, processes, and roles and responsibilities to maintain a comprehensive and accurate inventory of its data and corresponding metadata for its data types, as appropriate.	• Data inventory including data type, data classification, location, owner, retention requirements; • Metadata inventory; • Data flow Diagrams;

		In addition, the organization assigns data classifications to designated data types through tags or labels and appropriate metadata, such as provenance, data owner, geolocation, information location, etc., are tracked and maintained.	• System Configuration Documentation; • SOPs; • Evidence of Training-training records that demonstrate that staff responsible for data management have been trained on relevant policies and procedures;
		Managed and Measurable The organization ensures that the data and corresponding metadata in its inventories are subject to the monitoring processes defined within the organization's ISCM strategy. The organization uses data-centric security controls (e.g. DLP, encryption, rights management) in conjunction with data access controls (e.g., RBAC, CBAC, and ABAC) to secure data at every level and in every location.	• Data Quality Metrics-dashboards showing metrics related to data quality; • Data governance reports; • Audit logs; • Data Retention Schedules; • Incident Response Records-records of data related to security incidents.

		Optimized: The organization uses automation to develop and maintain a centralized data inventory that includes a mapping to the hardware and software components using or storing the data from all organizational information systems. The centralized inventory is updated in a near-real time basis In addition, the organization continuously discovers and analyzes ad hoc data to identify new instances of designated data types and updates its inventories accordingly	• Data Optimization Reports; • Technology Upgrade Plans; • Evidence of regular reviews of data policies and procedures.

Assessor Best Practices

Defined: Determine if the organization has established clear, documented procedures for data inventory management. This includes clearly defining data types and metadata requirements, and the data lifecycle stages.

Consistently Implemented: Assessors should ensure that standardized templates and processes are implemented across the organization to confirm consistency in data inventory practices.

Managed and measurable: Assessors review data inventory to ensure effective monitoring and oversight is implemented. Verify that the organization has mechanisms in place to track changes to data inventories, including additions, modifications, and deletions. Ensure effective management of these inventories requires regular updates and reviews to reflect changes in data assets and associated metadata.

Optimized: Determine whether the organization uses automated tools to develop and maintain a centralized data inventory that includes a mapping to the hardware and software components using or storing the data from all organizational information systems.

11. To what extent does the organization ensure that information system security risks are adequately managed?			
Criteria	**Review Cycle**	**Maturity Level**	**Suggested Standard Source Evidence**
• FISMA 2014 • EO 13800 • EO 14028 • OMB Circular A-123 • OMB Circular A-130 • OMB M-25-04 • OMB M-19-03 **Supplemental Guidance:**	Core	**Ad Hoc** The organization has not defined and communicated the policies, procedures and processes it uses to manage the cybersecurity risks associated with operating and maintaining its information systems. At a minimum, the policies, procedures, and processes do not cover the following areas from a cybersecurity perspective: • Prepare • Categorize • Select • Implement • Assess • Authorize • Monitor	

• NIST CSF v2.0: ID.RA-01 • NIST CSF v2.0: ID.RA-05 • NIST CSF v2.0: ID.RA-06 • NIST SP 800-53 (Rev. 5): RA-3 and PM-9 • NIST SP 800-37 (Rev. 2): Tasks P-2, P-3, P-14, R-2, and R-3 • NIST SP 800-39 • NIST IR 8286 • NIST IR 8286A • NIST IR 8286B • NIST IR 8286C • NIST IR 8286D		**Defined** The organization has defined and communicated the policies, procedures and processes it uses to manage the cybersecurity risks associated with operating and maintaining its information systems. The policies, procedures, and processes cover cybersecurity risk management at the organizational, mission/business process, and information system levels and address the following components • Prepare • Categorize • Select • Implement • Assess • Authorize • Monitor	• Enterprise Risk Management policies, procedures, and strategies; • Cybersecurity Risk Management policies, procedures, strategies; • Risk Assessment Policies and Procedures; • Insider Threat policies and procedures; • Data Breaches and Incident Response Polices and Procedures; • Cybersecurity training and awareness policies and procedures; • Ongoing Authorization policies and procedures; • System Categorization policies and procedures and SSPs; • SDLC policies and procedures; • EA policies and procedures; • Risk Executive Council Charters/delegations of authority; • POA&M policies and procedures; • Organizational risk profiles.

		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 uses the common vulnerability scoring system, or similar approach, to communicate the characteristics and severity of software vulnerabilities. Further, the organization uses a cybersecurity risk register to manage risks, as appropriate, and is consistently capturing and sharing lessons learned on the effectiveness of cybersecurity risk 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.

		Managed and Measurable 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.
		Optimized: The organization has maximized the use of automation, wherever possible, to increase the speed, effectiveness, and efficiency of	• Meeting minutes; • Email communications;

		steps associated with the risk management framework (e.g., prepare, categorize) The organization has achieved a real-time or near real-time risk-based decision-making process for managing cybersecurity risks.	• 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

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

12. 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**
• OMB Circular A-123 • OMB Circular A-130 • EO 14028 **Supplemental Guidance:** • NIST CSF v2.0: GV. RM-03 • NIST CSF v2.0: GV.RM-06 • NIST SP 800-53 (Rev. 5): CA-5(1) and CA-7 • NIST SP 800-37 (Rev. 2) • NIST SP 800-39 • NIST SP 800-207: Tenets 5 and 7 • NIST IR 8286 • OMB Circular A-123 • CISA Zero Trust Maturity Model: Pillars 2-4 • NIST IR 8286	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.
		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	• Risk Management documentation (ex. SSP/RAs, SARs, etc.); • Internal communications to stakeholders about risk (ex. emails, meeting minutes, etc.); • Enterprise wide POA&Ms;

		necessary sources of cybersecurity risk information are integrated into the solution.	• 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.; • Integrating SOAR to support GRC processes and functionality for real-time trend and analysis; • 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.

13. Provide any additional information on the effectiveness (positive or negative) of the organization's RAM 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 RAM 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:**			

Configuration Management			
14. To what extent does the organization use ***configuration settings/common secure configurations*** for its information systems?			
Criteria	**Review Cycle**	**Maturity Level**	**Suggested Standard Source Evidence**
• FISMA 2014 • OMB Circular A-130 • OMB M-25-04 • DHS BOD 23-01 • NIST FIPS 200 • OMB M-21-31 **Supplemental Guidance:** • NIST SP 800-70 (Rev. 4) • CIS Top 18 Security Controls: Controls 4 and 7 • CISA Cybersecurity Incident Response Playbooks • NIST CSF v2.0: ID.RA-01 • NIST CSF v2.0: PR.PS-01 • NIST Security Measures for EO-	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 baselining/hardening/configuration setting management, including processes for managing deviations; • Organization's tailored hardening guides.
		Consistently Implemented The organization consistently implements, assesses, and maintains secure configuration settings for its information systems based on the principle of least functionality.	• Evidence of vulnerability scanning conducted for the last four quarters; • Acceptable deviation/exception lists/justifications for organizationally tailored hardening guides;

Critical Software Use: SM 3.3 • NIST SP 800-53 (Rev. 5): CM-6, CM-7, RA-5, and SI-2 • OMB M-21-31, CISA Operational Guidance		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	• 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.

15. To what extent does the organization use flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities on all network addressable IP-assets?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• OMB M-25-04 • OMB Circular A-130 • NIST FIPS 200 • BOD 18-02 • BOD 19-02 • BOD 22-01 • BOD 23-01 **Supplemental Guidance:** • NIST CSF v2.0: ID.RA-01	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:	• Patch management/flaw remediation policies and procedures; • Configuration management policies and procedures; • BYOD policies and procedures.

• NIST SP 800-53 (Rev. 5): CM-3, RA-5, SI-2, and SI-3 • NIST SP 800-40 (Rev. 4) • NIST SP 800-207: Section 2.1 • NIST Security Measures for EO-Critical Software Use: SM 3.2 • FY 2025 CIO FISMA Metrics: 1.4, 8.1, and 8.2 • CIS Top 18 Security Controls: Controls 4 and 7 • BOD 23-01 Implementation Guidance • CISA Cybersecurity Incident Response Playbooks		- 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.	
		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. Further, for EO-critical software platforms and all software deployed to those platforms, the organization uses supported software versions.	• 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.
		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	• 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.

		software code, such as through patch sourcing and testing.	

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.

16. Provide any additional information (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 configuration management program effective?

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

Identity and Access Management (IDAM)			
17. 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 physical and logical assets [organization-defined entry/exit points], networks, and systems, including for remote access?			
Criteria	**Review Cycle**	**Maturity Level**	**Suggested Standard Source Evidence**
• Cybersecurity Enhancement Act of 2016 • OMB Circular A-130 • EO 14028 • FIPS 201-2 • HSPD-12 • OMB M-19-17 • OMB M-25-04 **Supplemental Guidance:** • NIST CSF v2.0: PR.AA-01 • NIST CSF v2.0: PR.AA-02 • 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	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.	
		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.	• Physical access control system configurations identifying strong authentication mechanisms on all defined protected entry/exit points in accordance with federal and agency-specific requirements;

• NIST SP 800-207: Tenet 6 • NIST Security Measures for EO-Critical Software Use: SM 1.1 • CIS Top 18 Security Controls: Control 6 • FY 2025 CIO FISMA Metrics: 2.3, 2.3.1, 2.3.2, 2.4, 2.9, 2.10, and 2.10.2		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.	• 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 Multifactor Authentication; • Plans for removal of passwords that require special characters or regular rotation, including in Mobile Device Management solutions.
		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.			

18. 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 physical and logical assets [organization-defined entry/exit points], networks, and systems, including for remote access?			
Criteria	**Review Cycle**	**Maturity Level**	**Suggested Standard Source Evidence**
• FIPS 201-2 • HSPD-12 • OMB M-19-17 • OMB M-25-04 • DHS ED 19-01	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	

Supplemental Guidance: • NIST CSF v2.0: PR.AA-01 • NIST CSF v2.0: PR.AA-02 • NIST SP 800-53 (Rev. 5): AC-17 and PE-3 • NIST SP 800-63 • NIST SP 800-128 • NIST SP 800-157 • NIST SP 800-207: Tenet 6 • NIST Security Measures for EO-Critical Software Use: SM 1.1 • CIS Top 18 Security Controls: Control 6 • FY 2025 CIO FISMA Metrics: 2.3, 2.4, 2.9, and 2.10		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.
		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 in accordance with federal and agency-specific requirements; • 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.
		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.

19. 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
• Cybersecurity Enhancement Act of 2016 • EO 14028 • OMB Circular A-130 • NIST FIPS 200 • OMB M-19-17 • OMB M-21-31 • DHS ED 19-01	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.

Supplemental Guidance: • NIST CSF v2.0: PR.AA-05 • 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 Security Measures for EO-Critical Software Use: SM 2.2 • FY 2025 CIO FISMA Metrics: 3.1 • CIS Top 18 Security Controls: Controls 5, 6, and 8		**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 (for example, UEBA reports, UAM reports). • 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.
		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	• Screenshots of automated tool or other mechanism that shows the management of privileged accounts and the automatic removal/disabling of temporary/emergency/inactive accounts.

		management logging requirements at maturity EL2, in accordance with M-21-31.	
		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:

20. Provide any additional information (positive or negative) of the organization's IDAM 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 IDAM 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:

Data Protection and Privacy

21. To what extent has the organization implemented the following security controls to protect the confidentiality, integrity, and availability of 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

• Backups of data are created, protected, maintained, and tested

• Access to personal email, external file sharing and storage sites, and personal communication applications are blocked, as appropriate. [DPP.01]			
Criteria	**Review Cycle**	**Maturity Level**	**Suggested Standard Source Evidence**
• OMB Circular A-130 • EO 14028 • DHS BOD 18-02 **Supplemental Guidance:** • NIST SP 800-37 (Rev. 2) • NIST SP 800-207 • NIST Security Measures for EO-Critical Software Use: SM 2.3 and SM 2.4 • DHS BOD 18-02 • CIS Top 18 Security Controls: Control 3 • FY 2025 CIO FISMA Metrics: 2.1, 2.1.1 and 2.2 • NIST CSF v2.0: PR.DS-01	Core	**Ad Hoc** The organization has not defined its policies and procedures in one or more of the specified areas.	

• NIST CSF v2.0: PR.DS-02 • NIST CSF v2.0: PR.DS-11 • NIST CSF v2.0: ID.AM-08			
		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, (iii) destruction or reuse, (iv) backup protection of media containing PII or other sensitive agency data, and (v) blocking of access to personal emails, external file storage sites, and personal communication applications.	• Evidence of database, file share, server, full disk encryption, 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;

			• Evidence of media backup protection; • Evidence of configurations or tools used to perform blocking of personal emails, external file storage sites, and personal communication applications.
		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.
		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; • Evidence of continuous backup of critical data in near real-time.

		• Continuously backing up critical data in near real-time.	

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:

22. To what extent has the organization implemented security controls (e.g., DLP, IDPS, CASB, User and Entity Behavior Analytic tools, SIEM and EDR) to prevent data exfiltration and enhance network defenses?

Criteria	Review Cycle	Maturity Level	Suggested Standard Source Evidence
• DHS BOD 18-01 • DHS ED 19-01 • OMB M-21-07 • OMB M-22-01 **Supplemental Guidance:** • CIS Top 18 Security Controls: Controls 9 and 10 • NIST CSF v2.0: DE.CM-01	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	
		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.

• NIST SP 800-53 (Rev. 5): SI-3, SI-7(8), SI-4(4)(18), SC-7(10), and SC-18 • NIST Security Measures for EO-Critical Software Use: SM 4.3 • FY2025 CIO FISMA Metrics: 10.8		**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 capabilities (e.g., using DLP, IDPS, CASB, User and Entity Behavior Analytic tools, SIEM and EDR tools) 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; • Evidence of tools used to support host-level visibility, attribution, and response for its information systems.
		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.	• Data exfiltration and network defense performance measure reports/dashboards; • After-action reports/meeting minutes from exfiltration exercises;

		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 solution deployments (e.g., using DLP, IDPS, CASB, User and Entity Behavior Analytic tools, SIEM and EDR tools).	• Evidence that DNS infrastructure is monitored in accordance with ISCM strategy; • Evidence of qualitative and quantitative measures on the performance of capabilities or tools used to support host-level visibility, attribution, and response for its information systems.
		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 DLP, IDPS, CASB, User and Entity Behavior Analytic tools, SIEM and 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, • Evidence of continuous device posture assessments.
Assessor Best Practices			
Defined: **Consistently Implemented:** **Managed and measurable:**			

Optimized:

23. Provide any additional information (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			
24. To what extent does the organization use an ***assessment of the skills, knowledge, and abilities of its workforce*** to provide specialized security training within the functional areas of: govern, identify, protect, detect, respond, and recover?			
Criteria	**Review Cycle**	**Maturity Level**	**Suggested Standard Source Evidence**
• Federal Cybersecurity Workforce Assessment Act of 2015 • Cybersecurity Enhancement Act of 2016 • EO 13870 • FISMA 2014 **Supplemental Guidance:** • NIST SP 800-50 Rev. 1: Section 3.2 • NIST SP 800-53 (Rev. 5): AT-2, AT-3, and PM-13 • NIST SP 800-181	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 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.
		Consistently Implemented The organization has assessed the knowledge, skills, and abilities of its workforce; tailored its specialized training; and has identified its skill gaps. Further, the organization periodically updates its assessment to account for a changing risk environment.	• 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;

• National Cybersecurity Workforce Framework • CIS Top 18 Security Controls: Control 14 • FY 2025 CIO FISMA Metrics: 6.1		In addition, the assessment serves as a key input to updating the organization's awareness and training strategy/plans.	• 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.

25. Provide any additional information (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	•
		Consistently Implemented	•

		Managed and Measurable	•
		Optimized:	•

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

<table>
<tr><th colspan="4">Information Security Continuous Monitoring (ISCM)</th></tr>
<tr><td colspan="4">26. 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?</td></tr>
<tr><th>Criteria</th><th>Review Cycle</th><th>Maturity Level</th><th>Suggested Standard Source Evidence</th></tr>
<tr><td rowspan="2">FISMA 2014
OMB Circular A-130
OMB M-25-04
NIST FIPS 200
Supplemental Guidance:
NIST SP 800-53 (Rev. 5): CA-7, PM-6, PM-14, and PM-31
NIST SP 800-37 (Rev. 2): Task P-7
NIST SP 800-137: Sections 3.1 and 3.6
NIST Security Measures for EO-Critical Software Use: SM 4.2
CIS Top 18 Security Controls: Control 13</td><td>Core</td><td><u>Ad Hoc</u>
The organization has not developed, tailored, and communicated its ISCM policies and an organization wide ISCM strategy.</td><td></td></tr>
<tr><td></td><td><u>Defined</u>
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</td><td>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.</td></tr>
</table>

		• Analyzing ISCM data, reporting findings, and reviewing and updating the ISCM policies, procedures, and strategy.	
		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).

		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.

27. To what extent does the organization monitor and measure the integrity and security posture of all owned and associated assets?			
Criteria	**Review Cycle**	**Maturity Level**	**Suggested Standard Source Evidence**
• OMB M-19-03 • OMB M-21-31 • EO 14028 • OMB Circular A-130 **Supplemental Guidance:** • NIST CSF v2.0: DE.CM-09 • NIST CSF v2.0: DE.AE-02 • NIST SP 800-53, Rev. 5: AU-12, CA-7, CM-10, CM-11, SC-34, SC-35, SI-4, and SI-7 • NIST SP 800-171 Rev. 3 • CIS Critical Security Controls v8: 8.11 • CIS Critical Security Controls v8: 10.1 • CISA Zero Trust Maturity Model	FY 2025 Supplemental	**Ad Hoc** The organization has not defined its policies and procedures to monitor and measure the integrity and security posture of all owned and associated assets.	
		Defined The organization has defined its policies and procedures to monitor and measure the integrity and security posture of all owned and associated assets	• Information security program policy; • ISCM strategy, policies, and procedures; • Organizational charts; • Delegations of authority; • Defined roles and responsibilities.
		Consistently Implemented The organization consistently analyzes the data it collects on potentially adverse events to better understand associated activities. The agency consistently implements monitoring and enforcement mechanisms to identify and manually disconnect or isolate non-compliant devices and virtual assets. The agency employs network monitoring capabilities based on known indicators of compromise to develop situational	• 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.

		awareness and correlates telemetry from multiple sources for analysis and monitoring.	
		Managed and Measurable The organization uses up to date cyber threat intelligence in log analysis tools to improve detection accuracy and characterize threat actors, their methods, and indicators of compromise. Further, manual reviews are conducted for technologies that cannot be sufficiently monitored through automation. The organization automates both inventory collection (including endpoint monitoring on all standard user devices and anomaly detection to detect unauthorized devices	• 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 has institutionalized the implementation of advanced ISCM technologies for analysis of trends and identification of potentially adverse events and adjusts its ISCM processes and security measures accordingly. The organization continuously verifies insights and enforces compliance throughout the lifetime of devices and virtual assets. The agency integrates device, software, configuration, and vulnerability management across all agency environments, including for virtual assets. The organization employs more sophisticated approaches to continuous monitoring (e.g., combines audit logs with other sources of event data).	• 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.

28. To what extent does the organization performing ongoing (continuous monitoring) information system assessments to grant system authorizations, including developing and maintaining system security plans, and monitoring system security controls?			
Criteria	**Review Cycle**	**Maturity Level**	**Suggested Standard Source Evidence**
• OMB Circular A-130 • OMB M-14-03 • OMB M-19-03 • EO 14028 **Supplemental Guidance:** • NIST SP 800-53 (Rev. 5): CA-2, CA-5, CA-6, CA-7, PL-2, and PM-10 • NIST SP 800-18 • NIST SP 800-37, Rev. 2: Task S-5 • NIST SP 800-137: Section 2.2 • NIST IR 8011 • NIST IR 8397 • FY 2025 CIO FISMA Metrics: 1.1.3 and 1.1.4	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.

		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.
		Optimized: The organization's system level ISCM policies and strategies are fully integrated	• See assessor best practices below.

		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.	

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.

29. 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)			
30. To what extent has the organization implemented ***processes related to incident detection and analysis***?			
Criteria	**Review Cycle**	**Maturity Level**	**Suggested Standard Source Evidence**
• OMB M-20-04 • OMB M-21-31 • OMB M-22-01 • OMB M-24-04 **Supplemental Guidance:** • 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 v2.0: ID-AM-03, DE.AE-02-04 and 08, PR.DS-01, RS.MA-02-03, DE.CM-09 • CISA Cybersecurity Incident Response Playbooks • CIS Top 18 Security Controls: Control 17 • US-CERT Federal Incident Notification Guidelines	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 potential adverse events 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.
		Consistently Implemented	• Sample of incident tickets, including those submitted to US-CERT;

• FY 2025 CIO FISMA Metrics: 3.1, 10.4, 10.5, and 10.6		The organization consistently implements enterprise-wide policies, procedures, and processes for incident detection and analysis.
		
		In addition, the organization consistently uses its enterprise-wide 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 potential adverse events and indicators generated by, for example, the following enterprise-wide 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.
			• 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.
		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 M-21-31. 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 M-21-31. 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 M-21-31. Evaluate the implemented logging processes and procedures against the EL3 logging requirements of M-21-31 and CISA implementation guidance.

31. To what extent has the organization implemented ***processes related to incident handling***?			
Criteria	**Review Cycle**	**Maturity Level**	**Suggested Standard Source Evidence**
• OMB M-21-31 • OMB M-24-04 • EO 14028 **Supplemental Guidance:** • NIST SP 800-53 (Rev. 5): IR-4 • NIST SP 800-61 (Rev. 2) • NIST IR 8374 • NIST CSF v.2.0: RS.MI-01 and RS.MI-02 • CISA Cybersecurity Incident Response Playbooks • FY 2025 CIO FISMA Metrics: 10.4, 10.5, and 10.6	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.	
		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 enterprise-wide incident handling policies,	• Sample of incident tickets to obtain evidence that incident handling policies and procedures, containment strategies, and incident eradication processes were

		procedures, containment strategies, and incident eradication processes. In addition, the organization consistently implements enterprise-wide 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 protecting incident data and metadata at an enterprise-wide level and sharing lessons learned on the effectiveness of its incident handling policies and procedures and making updates as necessary.	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.
		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	• Observe technologies in use for dynamic reconfiguration of network devices in response to incident types.

		firewalls and gateways) to stop attacks, misdirect attackers, and to isolate components of systems.	
Assessor Best Practices			
Defined: **Consistently Implemented:** **Managed and measurable:** **Optimized:**			

32. Provide any additional information (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)			
33. 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**
• OMB Circular A-130 • OMB M-19-03 • FIPS 199 **Supplemental Guidance:** • NIST CSF v2.0: ID.RA-04 • NIST SP 800-53 (Rev. 5): CP-2 and RA-9 • NIST SP 800-34 (Rev. 1): Section 3.2 • NIST IR 8179	Core	**Ad Hoc** Roles and responsibilities have not been fully defined and communicated across the organization, including appropriate delegations of authority.	
		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, such as its incident response plan, information system contingency plans, and continuity of operations plan (COOP).	• Information security strategy and policy; • Information system contingency planning strategy, policies, and procedures, including the requirements to use Business Impact.

• NIST IR 8286 • NIST IR 8286D • FCD-1 • FCD-2			• 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 • 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.
		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,	• Evidence that BIA results are integrated with organizational ERM processes; • Review meeting minutes supporting that the enterprise risk management

		recording, and monitoring the criticality and sensitivity of enterprise assets. As appropriate, the organization uses the results of its BIA in conjunction with its risk register to calculate potential losses and inform senior level decision making.	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:**			

34. 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**
• OMB Circular A-130 • OMB M-19-03 **Supplemental Guidance:** • NIST CSF v2.0: ID.IM-02 • NIST CSF v2.0: ID.IM-04 • NIST SP 800-53 (Rev. 5): CP-3 and CP-4 • NIST SP 800-34 • CIS Top 18 Security Controls: 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.
		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/Business Continuity Plan (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 that officials use 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., Information and Communications Technology (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.
		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:

35. 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:**			