FY 2022 Core IG FISMA Metrics Evaluation Guide

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 2022 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 is a companion document to the FY 2022 IG FISMA metrics[1] and provides guidance to IGs to assist in their FISMA evaluations.

Determining Effectiveness with Core Metrics

IGs must assess the effectiveness of information security programs on a maturity model spectrum. Aligning with the Carnegie Mellon Cybersecurity Maturity Model Certification (CMMI), the foundational levels require agencies to develop sound policies and procedures, while advanced levels capture the extent to which agencies institutionalize those policies and procedures.

Representatives from OMB, Federal Civilian Executive Branch (FCEB) CISO teams, CIGIE, and the Intelligence Community agreed these 20 Core IG Metrics should provide sufficient data to determine the effectiveness of an Agency's information security program with a high level of confidence.

As with previous guidance on the five-level maturity model, a Level 4, *Managed and Measurable,* information security program is still considered operating at an effective level of security. While determining effectiveness can be established based on the results of the IG metrics, IGs should continue to consider their own assessment of the unique missions, resources, and challenges faced by their agency when assessing the maturity of information security programs.

The tables below show the Core IG metrics for the FY 2022 IG evaluation period. These metrics were selected from the FY 21 IG metrics for their applicability to critical efforts emanating from Executive Order 14028 and OMB M-22-05.

[1] FY22 Core IG Metrics Implementation Analysis and Guidelines (cisa.gov)

Risk Management		
1. To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third-party systems), and system interconnections?		
Criteria	**Maturity Level**	**Suggested Standard Source Evidence**
• NIST SP 800-53. Rev. 5: CA-3 and PM-5 • NIST Cybersecurity Framework (CSF) ID.AM-1 – 4 • NIST SP 800-37, Rev. 2: Task P-18 • NIST 800-207, Section 7.3 • EO 14028, Section 3 • OMB A-130 • OMB M-22-05 • OMB M-22-09, Federal Zero Trust Strategy, Section B and D (5) • CISA Cybersecurity & Incident Response Playbooks • FY 2022 CIO FISMA Metrics: 1.1-1.1.5, 1.3	**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, inventories, strategies, and/or standards. These artifacts may relate to processes associated with maintaining the organization's information system inventory, using FISMA compliance tools (such as CSAM and RSAM) and other tools that may be deployed to capture component inventory information, infrastructure configuration management, SDLC, EA, or may be captured in a general Information Security Program policy.
	Consistently Implemented The organization maintains a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third-party systems), and system interconnections.	• An approved organization-wide information systems inventory • Approved program/division-level information systems inventories • Data Flow policies/procedures (to validate completeness) • Enterprise Architecture references (to validate completeness) • Final Interconnection Security Agreements

		(ISAs)/MOUs/MOAs/etc) to validate completeness • Agencies to provide any non.gov hostnames used to CISA and GSA ○ CISA will provide data about agencies' internet-accessible assets obtained through public and private sources (IGs can use this to evaluate public web app inventory) ○ Use of GSA website scanning service by IGs to assess inventory completeness[2]
	Managed and Measurable The organization ensures that the information systems included in its inventory are subject to the monitoring processes defined within the organization's ISCM strategy.	• ISCM strategy/plan • Continuous monitoring reports/dashboards • Change control requests • FedRAMP PMO communications • Web app domain registry information • EA documentation
	Optimized The organization uses automation to develop and maintain a centralized information system inventory that includes hardware and software components from all organizational information systems. The centralized inventory is updated in a near real time basis.	• Dashboard reports/observations • Hardware and software component inventories • Asset database reports • Examples of security alerts resulting from unauthorized hardware/software being placed on the network. • Evidence the reports and alerts are real-time

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

Additional notes:

At the defined level, IG evaluators should determine whether the agency's IT inventory asset management policies/procedures/processes address the addition of new systems and the retirement of old systems. IG evaluators should assess these policies and procedures to determine whether system boundary considerations (e.g., bundling) are outlined for inventorying.

At the consistently implemented level, and as part of the analysis performed by the IG evaluators for public facing web applications, utilize open-source tools/information (e.g., pulse.cio.gov) should identify the agencies subdomains and related services and compare against the inventory of information maintained by the agency for completeness and accuracy. The IG should also determine who approved the inventory.

At the managed and measurable level, IG evaluators 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.

At the optimized level, 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.

2. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?

Criteria	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-37, Rev. 2: Task P-10 and P-16 • NIST SP 800-53 Rev. 5: CA-7 and CM-8 • NIST SP 800-137 • NIST 800-207, 7.3.2 • NIST IR 8011 • Federal Enterprise Architecture (FEA) Framework, v2 • EO 14028, Section 3 • OMB M-22-05 • OMB M-22-09, Federal Zero Trust Strategy, Section B • CSF: ID.AM-1, ID.AM-5	**Ad Hoc** The organization has not defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting.	
	Defined The organization has defined policies, procedures, and processes for using standard data elements/taxonomy to	• Policies and procedures (and related guidance) for hardware asset management

• CISA Cybersecurity & Incident Response Playbooks • CIS Top 18 Security Controls v.8: Control 1 • FY 2022 CIO FISMA Metrics: 1.2-1.2.3	develop and maintain an up to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting.	• 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 and procedures • Information system component policies and procedures • Control baselines
	<u>Consistently Implemented</u> The organization consistently utilizes its standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network and uses this taxonomy to inform which assets can/cannot be introduced into the network.	• Authorized hardware inventory (which includes servers, mobile devices, endpoints, and network devices) • Agency SSPs • Information System Component Inventories (to validate the completeness of the hardware inventory by reconciling the Information System Component Inventories against the hardware inventory) • Continuous monitoring reports (e.g., vulnerability scanning reports, Splunk logs/reports, SCCM reports, etc.) listing of the hardware purchases • Enterprise Architecture documents

		• Inventory dashboards • Firewall configurations/logs • Configuration Management Data Base dashboards/reports.
	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.	• Scans configured to cover all agency networks and IP ranges (to validate completeness) • Continuous monitoring reports/dashboards (e.g., Splunk) • ISCM reports • FISMA compliance tools (such as CSAM and RSAM) • CDM reports, etc. • Mobile device management implementation
	Optimized The organization employs automation to track the life cycle of the organization's hardware assets with processes that limit the manual/procedural methods for asset management. Further, hardware inventories are regularly updated as part of the organization’s enterprise architecture current and future states.	• Hardware asset management reports (e.g., ServiceNow, CSAM, Forescout, CounterACT, BigFix reports) • MaaS configuration/reports • Continuous monitoring reports/dashboards (e.g., Splunk), • CDM reports • Enterprise Architecture documentation/reports

Additional notes:

At the defined level, IG evaluators 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 maintained. In addition, IG evaluators 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.

At the consistently implemented level, determine if the agency can reconcile its hardware asset inventory to the assets live on its network. The organization ensures 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. Please note, the sample should include assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. The sample should 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).

At the managed and measurable level, 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.

At the optimized level, determine whether the organization uses automated tools for hardware asset management, such as ServiceNow, CSAM, Forescout, CounterACT, BigFix, etc. For sampled systems, determine whether the hardware asset information in the automated tools is accurate and complete.

3. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?

Criteria	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-37, Rev. 2: Task P-10 and P-16 • NIST SP 800-53 Rev. 5: CA-7, CM-8, CM-10 and CM-11 • NIST SP 800-137 • NIST 800-207, Section 7.3 • NIST IR 8011 • FEA Framework, v2	**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 mobile applications, utilized in the	

• FY 2022 CIO FISMA Metrics: 1.3 and 4.0 • EO 14028, Section 4 • OMB M-21-30 • OMB M-22-05 • OMB M-22-09, Federal Zero Trust Strategy, Section B • CSF: ID.AM-2 • CISA Cybersecurity & Incident Response Playbooks • CIS Top 18 Security Controls v.8: Control 2	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 mobile applications, utilized in the organization's environment with the detailed information necessary for tracking and reporting.	• Policies and procedures (and related guidance) for software/license/asset management • Software naming standards/standard taxonomy document • Standard software images for devices • BYOD policies and procedures (e.g., mobile app rules) • Enterprise Architecture bricks • Scanning policies and procedures • Information system component policies and procedures • Change control policies and procedures • ISCM policies and procedures • SOPs for: - use of automation to maintain application inventories - protect against unwanted software, and - licensing conformance, etc. • Procedures for managing license restrictions and aging to ensure compliance with license limitations and constraints

		• Procedures for managing software licenses to ensure effective utilization, etc.
	<u>**Consistently Implemented**</u> The organization consistently utilizes its standard data elements/taxonomy to develop and maintain an up to-date inventory of software assets and licenses, including for mobile applications, utilized in the organization's environment and uses this taxonomy to inform which assets can/cannot be introduced into the network.	• Authorized software inventory • Agency SSPs • Information System Component Inventories (to validate the completeness of the software inventory by reconciling the Information System Component Inventories against the software inventory) • Continuous monitoring reports (e.g., vulnerability scanning reports, Splunk logs/reports, SCCM reports, etc.) listing of the software assets • Enterprise Architecture documents • Inventory dashboards • Firewall configurations/logs • CMDB dashboards/reports • Software license inventory listing, whitelisting/blacklisting tool (e.g., Applocker) system configurations, etc.
	<u>**Managed and Measurable**</u> The organization ensures that the software assets, including 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	• Authorized software inventory • Scans that gather device profiles and update information on software assets/licenses (to validate completeness) • Continuous monitoring reports/dashboards • ISCM strategy

	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).	• 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 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, • Network scanning reports • MaaS configurations, reports, dashboards, etc. • EA documentation • Software inventory
Additional notes: **At the defined level**, IG evaluators 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, IG evaluators 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. **At the consistently implemented level**, the agency can reconcile its software asset inventory to the assets live on its network. 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. **At the managed and measurable level**, 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 organization's allow listing technology ensures that only authorized software libraries may load into a system process.

At the optimized level, IG evaluators should obtain evidence [ex. network scanning reports designed to identify all instances of software, including 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.

5. To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels?

Criteria	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-37 (Rev. 2): Tasks P-2, P-3, P-14, R-2, and R-3 • NIST SP 800-39 • NIST SP 800-53, Rev. 5: RA-3 and PM-9 • NIST IR 8286 • OMB A-123 • OMB M-16-17 • OMB M-17-25 • CSF: ID RM-1 – ID.RM-3	**Ad Hoc** The organization has not defined and communicated the policies, procedures and processes it utilizes to manage the cybersecurity risks associated with operating and maintaining its information systems. At a minimum, the policies, procedures, and processes do not cover the following areas from a cybersecurity perspective: - Risk Framing - Risk assessment - Risk response - Risk monitoring	
	Defined The organization has defined and communicated the policies, procedures and processes it utilizes to manage the cybersecurity risks associated with operating and maintaining its information systems. The policies, procedures, and processes cover cybersecurity risk management at the	• Risk Management policies, procedures, and strategies • Risk Assessment Policies and Procedures • Ongoing Authorization policies and procedures • System Categorization policies and procedures • SDLC policies and procedures

	organizational, mission/business process, and information system levels and address the following components: - Risk Framing - Risk assessment - Risk response - Risk monitoring	• EA policies and procedures • Risk Executive Council Charters/delegations of authority • POA&M policies and procedures • Organizational risk profiles, • SSPs
	Consistently Implemented The organization consistently implements its policies, procedures, and processes to manage the cybersecurity risks associated with operating and maintaining its information systems. The organization ensures that decisions to manage cybersecurity risk at the information system level are informed and guided by risk decisions made at the organizational and mission/business levels. System risk assessments are performed [according to organizational defined time frames] and appropriate security controls to mitigate risks identified are implemented on a consistent basis. The organization utilizes the common vulnerability scoring system, or similar approach, to communicate the characteristics and severity of software vulnerabilities. Further, the organization utilizes a cybersecurity risk	• Risk Management policies, procedures, and strategies • 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 • Risk heat maps • POA&Ms • Project plans/taskers • Risk Council/steering committee meeting minutes • Investment Review meeting minutes/taskers

	register to manage risks, as appropriate, and is consistently capturing and sharing lessons learned on the effectiveness of cybersecurity risk management processes and updating the program accordingly.	• Lessons learned documents
	Managed and Measurable The organization utilizes the results of its system level risk assessments, along with other inputs, to perform and maintain an organization-wide cybersecurity and privacy risk assessment. The result of this assessment is documented in a cybersecurity risk register and serve as an input into the organization’s enterprise risk management program. The organization consistently monitors the effectiveness of risk responses to ensure that risk tolerances are maintained at an appropriate level. The organization ensures that information in cybersecurity risk registers is obtained accurately, consistently, and in a reproducible format and is used to (i) quantify and aggregate security risks, (ii) normalize cybersecurity risk information across organizational units, and (iii) prioritize operational risk response.	• Organization-wide risk assessment(s), • cyber risk registers, • 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.

	Optimized The cybersecurity risk management program is fully integrated at the organizational, mission/business process, and information system levels, as well as with the entity's enterprise risk management program. Further, the organization's cybersecurity risk management program is embedded into daily decision making across the organization and provides for continuous identification and monitoring to ensure that risk remains within organizationally defined acceptable levels. The organization utilizes Cybersecurity Framework profiles to align cybersecurity outcomes with mission or business requirements, risk tolerance, and resources of the organization.	• Meeting minutes; • email communications; • cyber risk register updates; • system workflow results/interactions; • investment/staffing documentation updates; • strategic planning documentation updates; • updates to the security program documentation - such as - updates to ISCM documentation, system security plans, system risk assessments; • updates to security performance metrics; • updates to system security plans; • updates to Business Impact Assessment/COOP documents; • NIST Cybersecurity Framework current/future state documentation; etc.
Additional notes: **At the defined level**, 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. **At the consistently implemented level**, IG evaluators 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, and these can determine if the organization has implemented security commensurate with the risk to the organization's mission and operations. **At the managed and measurable level**, IG evaluators 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.

At the optimized level, The IG evaluators should obtain artifacts evidencing that the organization utilizes Cybersecurity Framework profiles to align cybersecurity outcomes with mission or business requirements, risk tolerance, and resources of the organization.

10. To what extent does the organization utilize technology/ automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?

Criteria	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-39 • NIST 800-207, Tenets 5 and 7 • NIST IR 8286 • OMB A-123 • OMB M-22-09, Federal Zero Trust Strategy, Security Orchestration, Automation, and Response • CISA Zero Trust Maturity Model, Pillars 2-4	**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	• Risk Management documentation (ex. SSP/RAs, SARs, etc.)

	consistently implements an automated solution across the enterprise that provides a centralized, enterprise-wide view of cybersecurity risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. All necessary sources of cybersecurity risk information are integrated into the solution.	• Internal communications to stakeholders about risk (ex. emails, meeting minutes, etc.) • Enterprise wide POA&Ms • System level POA&Ms • GRC dashboards/reports
	Managed and Measurable The organization uses 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. 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 • 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	• Enterprise risk profiles • Enterprise-wide and component-level risk management dashboards • Budget/investment/staffing documentation

	cybersecurity risk management program.	• 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.
<u>Additional notes:</u> **At the defined level,** IG evaluators 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. **At the consistently implemented level,** the IG evaluators 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. **At the managed and measurable level,** the IG evaluators 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. **At the optimized level,** the IG evaluators 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.		

<table>
<tr><th colspan="3">Supply Chain Risk Management (SCRM)</th></tr>
<tr><td colspan="3"><b>14.</b> 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?</td></tr>
<tr><th>Criteria</th><th>Maturity Level</th><th>Suggested Standard Source Evidence</th></tr>
<tr><td>• The Federal Acquisition Supply Chain Security Act of 2018
• NIST SP 800-53, Rev. 5: SA-4, SR-3, SR-5 and SR-6 (as appropriate)
• NIST SP 800-152
• NIST 800-218, Task PO.1.3
• NIST IR 8276
• OMB A-130
• OMB M-19-03
• CSF: ID.SC-2 through 4
• FY 2022 CIO FISMA Metrics: 7.4.2
• CIS Top 18 Security Controls v.8: Control 15
• FedRAMP standard contract clauses; Cloud Computing Contract Best Practices</td><td><b><u>Ad Hoc</u></b>
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.</td><td></td></tr>
<tr><td></td><td><b><u>Defined</u></b>
The organization has defined and communicated policies and procedures to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements.

The following components, at a minimum, are defined
- The identification and prioritization of externally provided systems, system components, and services as well how the organization maintains awareness of its upstream suppliers
- Integration of acquisition processes, including the use of contractual agreements that stipulate appropriate cyber and SCRM measures for external providers.</td><td>• Policies, procedures, and processes that indicate how and what products, components, systems, and services will be accepted into the organization under the organization SCRM strategy. Said documents address at least 80% of the required components.

• Evidence that the policies, procedures, and processes have been published, communicated, and prioritized to the organization, including communication with external shareholders.

• Evidence that the agency has communicated its policies, procedures, and processes for ensuring that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements, to all stakeholders (emails, list,</td></tr>
</table>

	- Tools and techniques to utilize the acquisition process to protect the supply chain, including, risk-based processes for evaluating cyber supply chain risks associated with third party providers, as appropriate. - Contract tools or procurement methods to confirm contractors are meeting their contractual SCRM obligations.	web links, forums, seminars, etc.)
	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, or other forms of evaluation, that the security and supply chain controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and applicable NIST guidance. Furthermore, the organization maintains visibility into its upstream suppliers and can consistently track changes in suppliers.	• Organizationally defined documentation showing SCRM requirements are being implemented to assess and review SCRM risks with suppliers and/or contractors. Said documents should be from all levels of the organization; observe evidence from the selected sample systems. >75% of sample systems would indicate CI. • Audit or test result checklists, reports, or other forms of official record showing the organization has evaluated contractors or other entities adhere to security and SCRM requirements. • Reports from upstream suppliers indicating changes in suppliers. • Requests for reports and responses from upstream suppliers on regular basis. • Evidence in form of recent audits, internal reports, recent system scans and reviews, along with coordination with other agencies.

	Managed and Measurable The organization uses qualitative and quantitative performance metrics (e.g., those defined within SLAs) to measure, report on, and monitor the information security and SCRM performance of organizationally defined products, systems, and services provided by external providers. In addition, the organization has incorporated supplier risk evaluations, based on criticality, into its continuous monitoring practices to maintain situational awareness into the supply chain risks.	• Defined qualitative and quantitative performance measures used to measure external providers is in the policy, procedures, and process. • Defined processes for collecting qualitative and quantitative metrics and evidence said metrics were communicated to all levels of the organization (websites, emails, etc..). • Change logs indicating qualitative and quantitative metrics results were incorporated with the latest policy, procedures, and process update • Recent scans and IR reports and trend analysis. • Evidence of a quality control process and procedures in place to ensure data supporting metrics are obtained accurately, consistently, and in a reproducible format. • Supply chain risk evaluations incorporated into the continuous monitoring program.
	Optimized The organization analyzes, in a near-real time basis, the impact of material changes to security and SCRM assurance requirements on its relationships with external providers and ensures that acquisition tools, methods, and processes are updated as soon as possible.	• SCRM assessment reports from external providers and evidence that reports have led to change within the organization acquisition tools, methods, and processes in near real-time. • Vulnerability scan results/reporting monitoring to ensure proper patch management.

Additional notes: N/A

Configuration Management (CM)		
20. To what extent does the organization utilize configuration settings/common secure configurations for its information systems?		
Criteria	**Maturity Level**	**Suggested Standard Source Evidence**
• NIST SP 800-53, Rev. 5: CM-6, CM-7, and RA-5 • NIST SP 800-70, Rev. 4 • EO 14028, Section 4, 6, and 7 • OMB M-22-09, Federal Zero Trust Strategy, Section D • OMB M-22-05 • CISA Cybersecurity & Incident Response Playbooks • CIS Top 18 Security Controls v.8, Controls 4 and 7 • CSF: ID.RA-1 and DE.CM-8 • FY 2022 CIO FISMA Metrics, Section 7, Ground Truth Testing	**Ad Hoc** The organization has not established policies and procedures for ensuring that configuration settings/common secure configurations are defined, implemented, and monitored.	
	Defined The organization has developed, documented, and disseminated its policies and procedures for configuration settings/common secure configurations. In addition, the organization has developed, documented, and disseminated common secure configurations (hardening guides) that are tailored to its environment. Further, the organization has established a deviation process.	• Policies and procedures for system hardening/configuration setting management, including processes for managing deviations • Organization's tailored hardening guides
	Consistently Implemented The organization consistently implements, assesses, and maintains secure configuration settings for its information systems based on the	• Evidence of vulnerability scanning conducted for the last 4 quarters • Observation and analysis of Security Content Automation Protocol (SCAP) tools to determine coverage and use of rulesets and frequencies

	principle of least functionality. Further, the organization consistently utilizes SCAP-validated software assessing (scanning) capabilities against all systems on the network (see inventory from questions #1 - #3) to assess and manage both code-based and configuration-based vulnerabilities. The organization utilizes lessons learned in implementation to make improvements to its secure configuration policies and procedures.	- 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	- Evidence of frequent, enforced system configurations - Evidence of event-triggered configuration, Automated configuration from Continuous Diagnostics and Mitigation (CDM) events

	organization, or on an event driven basis.	- Automated routing/approval process and queues to enforce process and prevent out-of-sequence events

Additional notes:

At the defined level, IG evaluators should verify that the organization maintains security configuration standards for all authorized network devices (CIS Control 11.1). Further, IG evaluators should verify that the organization maintains documented security configuration standards for all authorized operating systems and software (CIS Control 5.1), including web servers. In addition, IG evaluators 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).

At the consistently implemented level, for a sample of systems, IG evaluators 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. IG evaluators may observe the tools used by the organization to conduct vulnerability scanning and verify the use of credentialed scans and coverage of devices/applications. IG evaluators should also analyze tool settings to verify coverage of scanning, rulesets, and schedules. IG evaluators 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 utilizing 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). IG evaluators should verify that the organization is using up to date SCAP compliant scanning tools. In addition, at Level 3, IG evaluators should verify that vulnerabilities identified through scanning activities, including for public facing web applications, are consistently remediated for sampled systems.

At the managed and measurable level, the organization should use automation, such as system configuration management tools to measure the security configurations of the devices connected to its network. 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 where deviations are identified. The intent at level 4 is to verify that the agency has readily available visibility into the security configurations (patch levels, implementation of hardening guides, vulnerabilities) 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.

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

21. To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities?		
Criteria	**Maturity Level**	**Suggested Standard Source Evidence**
• NIST SP 800-40, Rev. 3 • NIST SP 800-53, Rev. 5: CM-3, RA-5, SI-2, and SI-3 • NIST 800-207, section 2.1 • EO 14028, Sections 3 and 4 • OMB M-22-09, Federal Zero Trust Strategy, Section D • DHS Binding Operational Directives (BOD) 18-02 • BOD 19-02 • BOD 22-01 • CISA Cybersecurity Incident and Vulnerability Response Playbooks • CIS Top 18 Security Controls v.8, Controls 4 and 7 • CSF: ID.RA-1 • FY 2022 CIO FISMA Metrics: Section 8	**Ad Hoc** The organization has not developed, documented, and disseminated its policies and procedures for flaw remediation, including for mobile devices (GFE and non- GFE).	
	Defined The organization has developed, documented, and disseminated its policies and procedures for flaw remediation, including for mobile devices. Policies and procedures include processes for: - identifying, reporting, and correcting information system flaws, - testing software and firmware updates prior to implementation, - installing security relevant updates and patches within organizational-defined timeframes, and - incorporating flaw remediation into the organization's configuration management processes.	• Patch management policies and procedures • Configuration management policies and procedures
	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.	• 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

	In addition, the organization patches critical vulnerabilities within 30 days and utilizes lessons learned in implementation to make improvements to its flaw remediation policies and procedures.	• Documentation showing lessons learned that were obtained from all levels of the organization 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 software code, such as through patch sourcing and testing.	• Evidence of automated patch management and software updates using trusted, verified repositories for all applications and network devices • Integration with ISCM and IR programs to account for and utilize all flaw discovery sources

Additional notes:

At the consistently implemented level, for a sample of systems, obtain and analyze evidence of the remediation of configuration-related vulnerabilities within established timeframes.

<table>
<tr><th colspan="3">Identity, Credential, and Access Management (ICAM)</th></tr>
<tr><td colspan="3"><b>30.</b> To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for non-privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?</td></tr>
<tr><th>Criteria</th><th>Maturity Level</th><th>Suggested Standard Source Evidence</th></tr>
<tr><td rowspan="3">• NIST SP 800-53, Rev. 5: AC-17, IA-2, IA-5, IA-8, and PE-3
• NIST SP 800-63
• NIST SP 800-128
• NIST SP 800-157
• NIST 800-207 Tenet 6
• FIPS 201-2
• EO 14028, Section 3
• OMB M-19-17
• OMB M-22-05
• OMB M-22-09 Federal Zero Trust Strategy, Section A (2)
• HSPD-12
• CSF: PR.AC-1 and 6
• CIS Top 18 Security Controls v.8: Control 6
• FY 2022 CIO FISMA Metrics: Section 2</td><td><b>Ad Hoc</b>
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.</td><td></td></tr>
<tr><td><b>Defined</b>
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.</td><td>• 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</td></tr>
<tr><td><b>Consistently Implemented</b>
The organization has consistently implemented strong authentication mechanisms for non-privileged users of the organization’s facilities [organization-defined</td><td>• Physical access control system configurations identifying strong authentication mechanisms on all defined protected entry/exit points
• E-authentication risk assessments for sample systems</td></tr>
</table>

	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.	• 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 o Phishing resistant MFA o Plans for removal of passwords that require special characters or regular rotation, including in Mobile Device Management solutions.
	<u>Managed and Measurable</u> All non-privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems and facilities [organization-defined entry/exit points].	• 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.
	<u>Optimized</u> 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	• 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.

	report on effectiveness on a nearly real-time basis.	

Additional notes:
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. **At the optimized level**, sample select systems and test whether AD/PIV-based single sign on is enabled and enforced.

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

Criteria	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-53, Rev. 5: AC-17 and PE-3 • NIST SP 800-63 • NIST SP 800-128 • NIST SP 800-157 • NIST 800-207 Tenet 6 • FIPS 201-2 • EO 14028, Section 3 • OMB M-19-17 • OMB M-22-05 • OMB M-22-09, Federal Zero Trust Strategy, Section A (2) • HSPD-12 • CSF: PR.AC-1 and 6 • DHS ED 19-01 • CIS Top 18 Security Controls v.8: Control 6 • FY 2022 CIO FISMA Metrics: Section 2	**Ad Hoc** The organization has not planned for the use of strong authentication mechanisms for privileged users of the organization’s facilities [organization-defined entry/exit points], systems, and networks, including for remote access. In addition, the organization has not performed digital identity risk assessments to determine which systems require strong authentication.	
	Defined The organization has planned for the use of strong authentication mechanisms for privileged users of the organization’s facilities [organization-defined entry/exit points], systems, and networks, including the completion of digital identity risk assessments.	• Project plan for implementation of strong authentication for privileged users • E-authentication risk assessment policy and procedures • Site security plans identifying defined entry/exit points that must be protected.

	Consistently Implemented The organization has consistently implemented strong authentication mechanisms for privileged users of the organization's facilities [organization-defined entry/exit points] and networks, including for remote access, in accordance with Federal targets. For instances where it would be impracticable to use the PIV card, the organization uses an alternative token (derived PIV credential) which can be implemented and deployed with mobile devices.	• Physical access control system configurations identifying strong authentication mechanisms on all defined protected entry/exit points • Digital identity risk assessments for sample systems • System security plan for sampled systems • OS-and domain-level (Active Directory or similar directory service) configuration settings related to strong authentication • Mobile device management configuration settings related to strong authentication • Observation of and/or screenshots for sample systems that show how a non-privileged user logs into the network and system. • Plans for centralized identity mgt systems ○ Phishing resistant MFA ○ Plans for removal of passwords that require special characters or regular rotation, including in Mobile Device Management solutions.
	Managed and Measurable All privileged users, including those who can make changes to DNS records, utilize 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 nearly 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
Additional notes: 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. Sample select systems and test whether AD/PIV-based login is enabled and enforced as well as physical access controls.		

32. To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts and ensuring that privileged user account activities are logged and periodically reviewed).		
Criteria	**Maturity Level**	**Suggested Standard Source Evidence**
- NIST SP 800-53, Rev. 5: AC-1, AC-2, AC-5, AC-6, AC-17; AU-2, AU-3, AU-6, and IA-4 - EO 14028, Section 8 - OMB M-19-17 - OMB M-21-31 - DHS ED 19-01 - CSF: PR.AC-4 - CIS Top 18 Security Controls v.8: Controls 5, 6, and 8	**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	- 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.

- FY 2022 CIO FISMA Metrics: 3.1	users' accounts.	
	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; limits the privileged functions that can be performed using remote access; and ensures that privileged user activities are logged and periodically reviewed.	- Observation/documentation of domain, operating system, and network device account settings for privileged accounts - Log review reports for privileged user accounts - Inventory of privileged user accounts by type - List of auditable events for privileged users by system type - List of users by type and role for sampled systems - Controls that limit the duration a privileged user can be logged in - Controls that limit the privileged functions during remote access.
	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.	- Screenshots of automated tool or other mechanism that shows the management of privileged accounts and the automatic removal/disabling of temporary/emergency/inactive accounts
Additional notes: 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. **Level 5, Optimized is not defined.**		

Data Protection & Privacy (DP&P)

36. To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle?

- Encryption of data at rest
- Encryption of data in transit
- Limitation of transfer to removable media
- Sanitization of digital media prior to disposal or reuse

Criteria	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-37 (Rev. 2) • NIST SP 800-53, Rev. 5; SC-8, SC-28, MP-3, and MP-6 • NIST 800-207 • EO 14028 Section 3(d); • OMB M-22-09, Federal Zero Trust Strategy • DHS BOD 18-02 • CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6 • CIS Top 18 Security Controls v. 8: Control 3 • FY 2022 CIO FISMA Metrics: 2.1, 2.2, 2.12, 2.13	**Ad Hoc** The organization has not defined its policies and procedures, at a minimum, in one or more of the specified areas.	
	Defined The organization's policies and procedures have been defined and communicated for the specified areas. Further, the policies and procedures have been tailored to the organization's environment and include specific considerations based on data classification and sensitivity.	• Information security, data life cycle, and/or protection policies and procedures • Data classification/handling policies and procedures • Privacy Plan, including policies and procedures
	Consistently Implemented The organization's policies and procedures have been consistently implemented for the specified areas, including (i) use of FIPS-validated encryption of PII and other agency sensitive data, as appropriate, both at rest and in transit, (ii) prevention and detection of untrusted removable media, and (iii) destruction or reuse of media containing PII or other sensitive agency data.	• Evidence of database, file share, server, and end point encryption where PII or sensitive information is stored • Evidence 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

		• Evaluate agency progress in deploying encrypted DNS • Plans for encryption of all http traffic within the environment • Preloading .gov domains into web browsers as only accessible via https (see https://home.dotgov.gov/management/preloading/ and https://hstspreload.org/
	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 (i) remote wiping, (ii) dual authorization for sanitization of media devices, and (iii) exemption of media marking if the media remains within organizationally defined control areas (iv) 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/creation/update/deletion/ destruction dates and confirmation that these fields are required. • Evidence of data storage/destruction in accordance with the data retention schedule
Additional notes: Encryption algorithms used to encrypt data at rest and in transit must be FIPS-validated.		

37. To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses?		
Criteria	**Maturity Level**	**Suggested Standard Source Evidence**
• NIST SP 800-53, Rev. 5: SI-3, SI-7, SI-4, SC-7, and SC-18 • OMB M-21-07 • DHS BOD 18-01 • DHS ED 19-01 • CSF: PR.DS-5, • CIS Top 18 Security Controls v.8: Controls 9 and 10 • FY 2022 CIO FISMA Metrics, 5.1	**Ad Hoc** The organization has not defined its policies and procedures related to data exfiltration, 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, enhanced network defenses, email authentication processes, and mitigation against DNS infrastructure tampering.	• Data exfiltration/network defense policies and procedures
	Consistently Implemented The organization consistently monitors inbound and outbound network traffic, ensuring that all traffic passes through a web content filter that protects against phishing, malware, and blocks against known malicious sites. Additionally, the organization checks outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII. Also, suspected malicious traffic is quarantined or blocked. In addition, the organization utilizes email authentication technology and ensures the	• 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 • Evidence of valid domain encryption certificates

	use of valid encryption certificates for its domains.	
	Managed and Measurable The organization analyzes qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses. The organization also conducts exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses. Further, the organization monitors its DNS infrastructure for potential tampering, in accordance with its ISCM strategy. In addition, the organization audits its DNS records.	• Data exfiltration and network defense performance measure reports/dashboards • After-action reports/meeting minutes from data exfiltration and enhanced network defense exercises. • Evidence that DNS infrastructure is monitored in accordance with ISCM strategy • DNS records audit results
	Optimized The organizations 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.	• ISCM strategy • Incident response plan • Evidence showing integration with other security domains, including configuration management, ISCM, and incident response
Additional notes: IGs should consider exfiltration and enhanced defenses for both email and web vectors separately, including the technologies, processes, and rules that apply. IGs should also evaluate data exfiltration protections and network defenses related to USB and other removable media.		

Security Training (ST)

42. To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover?

Criteria	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-50: Section 3.2 • NIST SP 800-53, Rev. 5: AT-2, AT-3, and PM-13 • NIST SP 800-181 • Federal Cybersecurity Workforce Assessment Act of 2015 • National Cybersecurity Workforce Framework v1.0 • CIS Top 18 Security Controls v.8: Control 14 • FY 2022 CIO FISMA Metrics, Section 6	**Ad Hoc** The organization has not defined its processes for assessing the knowledge, skills, and abilities of its workforce.	
	Defined The organization has defined its processes for assessing the knowledge, skills, and abilities of its workforce to determine its awareness and specialized training needs and periodically updating its assessment to account for a changing risk environment.	• Workforce assessment policies and procedures (or related documentation) • Security training policies and procedures
	Consistently Implemented The organization has assessed the knowledge, skills, and abilities of its workforce; tailored its awareness and specialized training; and has identified its skill gaps. Further, the organization periodically updates its assessment to account for a changing risk environment. In addition, the assessment serves as a key input to updating the organization's awareness and training strategy/plans.	• Cybersecurity Workforce assessment • Content of awareness and role-based training programs • Action plan to close gaps identified through its workforce assessment • Training Strategy/Plan(s)
	Managed and Measurable The organization has addressed its identified knowledge, skills, and	• Evidence that the agency has made progress in addressing gaps identified through its workforce assessment

	abilities gaps through training or talent acquisition.	
	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
Additional notes: N/A		

Information Security Continuous Monitoring (ISCM)		
47. To what extent does the organization utilize information security continuous monitoring (ISCM) policies and ISCM strategy that addresses ISCM requirements and activities at each organizational tier?		
Criteria	**Maturity Level**	**Suggested Standard Source Evidence**
• NIST SP 800-37 (Rev. 2) Task P-7 • NIST SP 800-53, Rev. 5: CA-7, PM-6, PM-14, and PM-31 • NIST SP 800-137: Sections 3.1 and 3.6 • CIS Top 18 Security Controls v.8: Control 13	**Ad Hoc** The organization has not developed, tailored, and communicated its ISCM policies and an organization wide strategy.	
	Defined The organization has developed, tailored, and communicated its ISCM policies and an organization wide 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	• ISCM strategy • ISCM policies and procedures • Agency-wide information security policy

	with organizational officials [e.g., senior accountable official for risk management, system owners, and common control providers] and in accordance with organizational risk tolerance. - The organization's ongoing control assessment approach - How ongoing assessments are to be conducted - Analyzing ISCM data, reporting findings, and reviewing and updating the ISCM policies, procedures, and strategy.	
	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 and assessment reports for selected systems • Evidence that agency dashboard exists with visibility of all organizational assets • Evidence of a lessons learned process
	Managed and Measurable The organization monitors and analyzes qualitative and quantitative performance measures on the	• Evidence of use of performance metrics/dashboards defined in the ISCM strategy

	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 verifications/validation of data feeding the metrics/dashboard • Evidence that control assessments were performed at frequency defined by ongoing assessment strategy/schedule. • Evidence of ongoing system authorizations for select systems (including 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.	• See additional guidance provided on the integration of ISCM into risk management. • Evidence supporting continuous monitoring tools and technologies are used in other security domains, including risk management, configuration management, incident response, and business continuity.
Additional notes: **At the defined level,** review the organization wide ISCM strategy and confirm the strategy has defined (1) the frequency at which implemented controls on organizational systems will be assessed, (2) how ongoing assessments will be carried out and at what frequency, and (3) a risk-based approach for security control assessment frequency selection. **At the consistently implemented level**, review evidence (e.g., reports or analysis output from an agency dashboard) that support control assessments occurring on an ongoing basis and continuous monitoring (e.g., known vulnerabilities, patches, etc...) in real time. Additionally, review agency dashboard screenshots (e.g., CDM or agency dashboard and/or SIEM etc..) that		

support the organization has visibility over asset vulnerabilities. Last, review reports or other analysis that support feedback is utilized to create lessons learned.

At the managed and measured level, 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 supports control assessments occur on the ongoing basis defined in the system's ISCM strategy, and (3) evidence that authorization decisions are based on the results of ongoing assessments. An organization cannot reach this maturity level until it has fully transitioned to ongoing control and system authorizations.

At the optimized level, the outputs of the ISCM process serve as inputs to the agency's enterprise and supply chain risk management, incident response, business continuity, configuration management, and other related programs on a near-real time basis.

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

Criteria	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-18, Rev. 1 • NIST SP 800-37 (Rev. 2) Task S-5 • NIST SP 800-53, Rev. 5: CA-2, CA-5, CA-6, CA-7, PL-2, and PM-10 • NIST SP 800-137: Section 2.2 • NIST IR 8011 • OMB A-130 • OMB M-14-03 • OMB M-19-03 • OMB M-22-09	**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	• ISCM strategy • ISCM policies and procedures • Agency-wide information security policy • System level continuous monitoring plan for selected systems.

	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.	
	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 ongoing system authorizations for select systems (including POA&Ms, SSPs, security assessment reports (SAR), and ATO letters) • Organization-wide risk management strategy, appetite, and tolerance • Use of dedicated application security testing programs • IG's can verify whether agency SAR process have been updated IAW M-22-09 (section III.D.1) to incorporate more time-sensitive, specialized, and application specific methods
	Managed and Measurable The organization utilizes the results of security control	• Evidence of the generation and collection of security-related information for all implemented

	assessments and monitoring to maintain ongoing authorizations of information systems, including the maintenance of system security plans.	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 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.	• At the optimized level, automated tools are used to support authorizing officials in making ongoing authorization decisions. Where automation is not feasible, manual or procedural security assessments are conducted to cover the gaps. Request any realized cost savings of continuous monitoring.
Additional notes: 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.		

Incident Response (IR)		
54. How mature are the organization's processes for incident detection and analysis?		
Criteria	**Maturity Level**	**Suggested Standard Source Evidence**
• NIST 800-53, Rev. 5: IR-4, IR-5, and IR-6 • NIST SP 800-61 Rev. 2 • EO 14028, Section 6 • OMB M-20-04 • OMB M-21-31 • OMB M-22-05, Section I;	**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,	

• CISA Cybersecurity Incident and Vulnerability Response Playbooks • CSF: DE.AE-1, DE.AE-2 -5, PR.DS-6, RS.AN-1 and 4, and PR.DS-8 • CIS Top 18 Security Controls v.8: Control 17 • US-CERT Incident Response Guidelines • FY 2022 CIO FISMA Metrics: 10.6	analyzing, and prioritizing incidents.	
	Defined The organization has defined and communicated its policies, procedures, and processes for incident detection and analysis. In addition, the organization has defined a common threat vector taxonomy and developed handling procedures for specific types of incidents, as appropriate. In addition, the organization has defined its processes and supporting technologies for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed, and for prioritizing incidents.	• Incident detection and analysis strategies, policies, procedures, and standards, including a common threat vector taxonomy • Enterprise-level incident response plan • Network architecture diagram highlighting the layers of protection/technologies in place to detect and analyze incidents • SOPs for supporting technologies used to detect/analyze potential incidents
	Consistently Implemented The organization consistently implements its policies, procedures, and processes for incident detection and analysis. In addition, the organization consistently utilizes its threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization. In addition, the organization consistently implements, and analyzes precursors and indicators generated by, for example, the following technologies: intrusion	• Sample of incident tickets, including those submitted to US-CERT • Evidence of configurations that show the precursors and indicators captured 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

	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.	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 req’s • Plans to meet the first event logging maturity level (EL-1) NLT than Aug 22, per M-21-31 • 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 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,	• 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

	consistently, and in a reproducible format. The organization utilizes 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.	
	Optimized N/A	
Additional notes: **At the consistently implemented level**, observe technologies and tools supporting incident detection and analysis to verify whether the defined indicators and precursors are being captured and reviewed.		

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

Criteria	Maturity Level	Suggested Standard Source Evidence
• NIST 800-53, Rev. 5: IR-4 • NIST SP 800-61, Rev. 2 • EO 14028, Section 6 • OMB M-22-05, Section I	**Ad Hoc** The organization has not defined its policies, procedures, and processes for incident handling to include containment strategies for various types	

- CISA Cybersecurity Incident and Vulnerability Response Playbooks - CSF: RS.MI-1 and 2 - FY 2022 CIO FISMA Metrics: 10.6	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 - Incident eradication, vulnerability mitigation, and system recovery processes and procedures
	Consistently Implemented The organization consistently implements its incident handling policies, procedures, containment strategies, and incident eradication processes. In addition, the organization consistently implements processes to remediate	- Sample of incident tickets to obtain evidence that incident handling policies and procedures, containment strategies, and incident eradication processes were followed - Evidence that vulnerabilities that were exploited and resulted in incidents were remediated

	vulnerabilities that may have been exploited on the target system(s) and recovers system operations. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident handling policies and procedures and making updates as necessary.	(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 utilizes dynamic reconfiguration (e.g., changes to router rules, access control lists, and filter rules for firewalls and gateways) to stop attacks, misdirect attackers, and to isolate components of systems.	• Observe technologies in use for dynamic reconfiguration of network devices in response to incident types.
Additional notes: N/A		

Contingency Planning (CP)		
61. To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts?		
Criteria	**Maturity Level**	**Suggested Standard Source Evidence**
- NIST SP 800-34, Rev. 1, 3.2 - NIST SP 800-53, Rev. 5: CP-2, and RA-9 - NIST IR 8286 - FIPS 199 - FCD-1 - OMB M-19-03 - CSF:ID.RA-4 - FY 2022 CIO FISMA Metrics: 10.1.4	**Ad Hoc** The organization has not defined its policies, procedures, and processes for conducting organizational and system level BIAs and for incorporating the results into strategy and plan development efforts.	
	Defined The organization has defined its policies, procedures, and processes for conducting organizational and system level BIAs and for incorporating the results into strategy and plan development efforts.	- Information security policy - Information system contingency planning policies and procedures - Business Impact Analysis policies, procedures, and processes
	Consistently Implemented The organization consistently incorporates the results of organizational and system level BIAs into strategy and plan development efforts. System level BIAs are integrated with the organizational level BIA and include characterization of all system components, determination of missions/business processes and recovery criticality, identification of resource requirements, and identification of recovery priorities for system resources. The results of the BIA are consistently used to determine contingency planning requirements and priorities, including mission	- Templates for completing BIAs - Organizational level BIA - Sample of system level BIAs

	essential functions/high value assets.	
	Managed and Measurable The organization ensures that the results of organizational and system level BIAs are integrated with enterprise risk management processes, for consistently evaluating, recording, and monitoring the criticality and sensitivity of enterprise assets. As appropriate, the organization utilizes the results of its BIA in conjunction with its risk register to calculate potential losses and inform senior level decision making.	• Evidence that BIA results are integrated with organizational ERM processes • Enterprise risk management meeting minutes showing the BIA was discussed.
	Optimized N/A	
Additional notes: N/A		

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

Criteria	Maturity Level	Suggested Standard Source Evidence
• NIST SP 800-34 • NIST SP 800-53, Rev. 5: CP-3 and CP-4; • CSF: ID.SC-5 and PR.IP-10 • CIS Top 18 Security Controls v.8: Control 11 • FY 2022 CIO FISMA Metrics: 10.1	**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	• Information security policy • Information system contingency planning policies and procedures

	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.	
	Consistently Implemented Information system contingency plan testing, and exercises are consistently implemented. ISCP testing and exercises are integrated, to the extent practicable, with testing of related plans, such as incident response plan/COOP/BCP.	• ISCP testing results for selected systems • Results of testing of COOP, BCP, DRP, and OEP • Evidence of after-action reports to improve the program from the exercise results
	Managed and Measurable The organization employs automated mechanisms to test system contingency plans more thoroughly and effectively. In addition, the organization coordinates plan testing with external stakeholders (e.g., ICT supply chain partners/providers), as appropriate.	• ISCP testing results for selected systems • Results of testing of COOP, BCP, DRP, and OEP • Coordination emails • AAR's showing 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 and show evidence of testing the effectiveness of the contingency planning process.

Additional notes: N/A