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, in coordination with the Office of Management and Budget, the Department of Homeland Security, and the Federal Chief Information Officers and Chief Information Security Officers councils are providing this evaluation guide for IGs to use in their 2019 FISMA evaluations.

The guide is designed to provide 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 2019 IG FISMA metrics (available at https://www.dhs.gov/publication/fy19-fisma-documents) and is intended to provide guidance to IGs to assist in their FISMA evaluations.

IG Metric - FY19	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
1. To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third party systems), and system interconnections (NIST SP 800-53.	**Ad Hoc** The organization has not defined a process to develop and maintain a comprehensive and accurate inventory of its information systems and system interconnections.		For Level 2, 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. Furthermore, IG evaluators should assess these policies and procedures to determine whether system boundary considerations (e.g., bundling) are outlined for inventorying purposes. IG evaluators should determine if the agency's policies/procedures clearly outline the requirements/processes for maintaining an inventory of information systems, including cloud solutions, third party systems, and public-facing web applications (see CIGIE Web Application Report at https://www.ignet.gov/sites/default/files/files/Web_Applications_Security_Cross-Cutting_Project.pdf for additional details). In addition, IG evaluators should verify that the agency's IT inventory asset management policies/procedures/processes address how the agency ensures the completeness and accuracy of its systems inventory.
	Defined The organization has defined, but not consistently implemented, a process to develop and maintain a comprehensive and accurate inventory of its information systems and system interconnections.	• Information System Inventory Standard/related policies and procedures for maintaining the organization's information system inventory • Information Security Program Policy • SOPs for use of FISMA compliance tools (such as CSAM and RSAM) and other tools that may be deployed to capture component inventory information • Infrastructure configuration management operating procedures • SDLC and EA policy and procedures • Inventory of information systems	
	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.	• Approved organization-wide information systems inventory • Approved component/division-level information systems inventories • Data Flow policies/procedures (to validate completeness) • Enterprise Architecture references (to validate completeness) • Interconnection Security Agreements (ISAs)/MOUs/MOAs (to validate completeness)	
	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 • Continuous monitoring reports/dashboards	

IG Metric - FY19	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
1. (Continued) To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third party systems), and system interconnections (NIST SP 800-53. Rev. 4: CA-3, PM-5, and CM-8; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2019 CIO FISMA Metrics: 1.1 and 1.4, OMB A-130).	**Optimized** The organization uses automation to develop 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.	• Observation/Testing of an automated centralized information system inventory	For level 4, IG evaluators should sample select systems from the organization's approved inventory to determine whether the organization's continuous monitoring processes have been implemented, including the capture and review of metrics defined within the ISCM strategy. Also, IG evaluators should determine whether the agency has timely access to information from the FedRAMP PMO to effectively perform continuous monitoring activities. Furthermore, for the agency's public facing websites and related subdomains and services, IG evaluators should determine whether domain registry information is continuously monitored and updated. Further, IG evaluators should review the organization's Architecture documentation and ensure that there are clear references to the organization's system inventory, and verify that changes to the organization's information system inventory are reflected in the organization's EA documentation/repository. For Level 4: IG evaluators should select a sample of new system implementations, system major modifications, and system decommissioning's, and ensure that these changes are reflected in the organization's Information System Inventory (completeness/accuracy). For level 5, sample select systems from the organization's approved inventory to determine whether the agency has the capability to automatically identify system hardware/software components and supply chain vendors and make updates in a near-real time fashion. At level 5, the organization's hardware and software component inventories are integrated so that all devices are tracked from a central location. IG evaluators should place a sample of "unauthorized" devices on various portions of the organization's network unannounced to ensure these devices are detected, quarantined, and removed in a timely manner (parameters/metrics (timeframes) should be defined by the organization's ISCM program): o The devices should be placed on multiple subnets o The devices should be in the asset inventory database o The devices should be detected within 24 hours (or within the organization-defined timeframe, if this timeframe differs from the 24 hour best practice indicated) o The devices should be isolated within 1 hour of detection (or within the organization-defined timeframe if this timeframe differs from the 1 hour best practice indicated) o The details regarding location and department where the devices were placed should be recorded (SANS Institute Realistic Risk Management Using the CIS 20 Security Controls)

IG Metric - FY19	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
2. To what extent does the organization use 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 (NIST SP 800-53 Rev. 4: CA-7 and	**Ad Hoc** The organization has not defined a process 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.		At Level 2, IG evaluators should obtain organizational policies and procedures that address the development and maintenance of a comprehensive, accurate, and up-to-date inventory of organizational hardware assets. The policies and procedures should address the following: • The process employed by the organization to identify and document/inventory all agency hardware assets (CSC-1). • The process employed by the organization to ensure that only authorized hardware assets are given access, and unauthorized/unmanaged hardware assets are found and prevented from gaining access (CSC-1). • The organization-defined timeframe management must isolate and remove the identified devices from the network (SANS Institute Realistic Risk Management Using the CIS 20 Security Controls).
	Defined The organization has defined, but not consistently implemented, a process 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.	• Policies and procedures (and related guidance) for hardware asset management, including approval processes for purchases. • Hardware naming standards/standard taxonomy document • End user computing device inventory standards • Enterprise architecture bricks	
	Consistently Implemented 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.	• Hardware inventory (which includes servers, mobile devices, endpoints, and network devices) • Agency SSPs (to validate completeness of the inventory though reconciliations of the Information System Component Inventories against the hardware inventory)	
	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.	• Scans that are configured to cover all agency networks and IP ranges (to validate completeness) • Continuous monitoring reports/dashboard • ISCM strategy	
	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.	• Scanning and alert results, which update the solution used to track hardware throughout its lifecycle on a near-real time basis • Asset tagging and documentation	

IG Metric - FY19	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
2. (Continued) To what extent does the organization use 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 (NIST SP 800-53 Rev. 4: CA-7 and CM-8; NIST SP 800-137; NISTIR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2019 CIO FISMA Metrics: 1.2 and 3.9.2; CSF: ID.AM-1).			At level 4, sample select systems and verify that hardware assets are subject to the organization's continuous monitoring processes. Verify that metrics are used to manage and measure the implementation of the organization's ISCM processes for the hardware assets sampled. IG evaluators should place a sample of “unauthorized” devices on various portions of the organization’s network, preferably unannounced, to ensure these devices are detected, quarantined, and removed in a timely manner (parameters/metrics (timeframes) should be defined by the organization's ISCM program): o The devices should be placed on multiple subnets o The devices should be in the asset inventory database o The devices should be detected within 24 hours (or within the organization-defined timeframe, if this timeframe differs from the 24 hour best practice indicated) o The devices should be isolated within 1 hour of detection (or within the organization-defined timeframe if this timeframe differs from the 1 hour best practice indicated) o The details regarding location and department where the devices were placed should be recorded (SANS Institute Realistic Risk Management Using the CIS 20 Security Controls) In addition, determine whether the organization has deployed its hardware asset management tool/capability to selected hardware devices supporting sampled systems Furthermore, determine whether the agency has standardized reporting and inventory processes to effectively implement the hardware asset management module of CDM. At level 5, 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. For assets that have been decommissioned, the organization utilizes automation to update, in near real-time, the status of these devices in its hardware asset inventory. Furthermore, the organization uses client certificates to authenticate hardware assets connecting to its trusted network (See CIS Controls v 7.1, #1.8). IG evaluators should determine if 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.

IG Metric - FY19	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
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 (NIST SP 800-53 Rev. 4: CA-7, CM-8, and CM-10; NIST SP 800-137;	**Ad Hoc** The organization has not defined a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses utilized in the organization's environment with the detailed information necessary for tracking and reporting.		At level 2, IG evaluators should determine whether the agency's IT asset management policies and procedures define the requirements and processes for software asset management, including the standard data elements/taxonomy that are 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 roles and responsibilities. The organization's policies and supporting procedures should define how it maintains an up-to-date inventory of the software assets connected to its network, the associated licenses, and how information is tracked and reported. At level 2, IG evaluators should obtain organizational policies and procedures that address the development and maintenance of a comprehensive, accurate, and up-to-date inventory of organizational software and software licenses. The policies and procedures should, at a minimum address the processes: • employed by the organization to identify and document/inventory all agency software and software licenses (CSC-2).
	Defined The organization has defined, but not consistently implemented, a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses 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 • Standard software image for devices • Enterprise architecture bricks	
	Consistently Implemented The organization consistently utilizes its standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses utilized in the organization's environment and uses this taxonomy to inform which assets can/cannot be introduced into the network.	• Software inventory • Agency SSPs (to validate completeness of the inventory though reconciliations of the Information System Component Inventories against the software Inventory) • Software license inventory listing • SOPs around use of automation to maintain application inventories, protect against unwanted software, and licensing conformance • Procedures for managing license restrictions and aging to ensure compliance with license limitations and constraints • Procedures for managing software licenses to ensure effective utilization	
	Managed and Measurable The organization ensures that the software assets on the network (and their associated licenses) are covered by an organization-wide software asset management capability and are subject to the monitoring processes defined within the organization's ISCM strategy.	• Scans that gather device profiles and update information on software assets/licenses (to validate completeness) • Continuous monitoring reports/dashboard • ISCM strategy	
	Optimized The organization employs automation to track the life cycle of the organization's software assets (and their associated licenses) 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 update the solution used to track software throughout its lifecycle on a near-real time basis	

IG Metric - FY19	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
3. (Continued) 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 (NIST SP 800-53 Rev. 4: CA-7, CM-8, and CM-10; NIST SP 800-137; NISTIR 8011; FEA Framework, v2; FY 2019 CIO FISMA Metrics: 3.10.1; CSF: ID.AM-2)?			At level 4, the agency has deployed application whitelisting technology on all assets, as appropriate, to ensure that only authorized software executes and all unauthorized software is blocked from executing. The organization's whitelisting technology ensures that only authorized software libraries are allowed to load into a system process (CIS V. 7.1, #2.8). Further, at level 4, sample select systems to ensure that system software applications are subject to the organization's ISCM processes. In addition, determine whether the organization has deployed its software asset management tool/capability to selected to sampled systems. Furthermore, determine whether the agency has standardized reporting and inventory processes to effectively implement the software asset management module of CDM. At level 4, determine if the organization's continuous monitoring processes ensure that only software applications and operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be noted as such in the inventory system (CIS V. 7.1, #2.2). At level 4, IG evaluators may install a sample of “unauthorized” instances of different types of software on each of the various organizational platforms unannounced to ensure this software is detected, quarantined, and removed in a timely manner (parameters/metrics (timeframes) should be defined by the organization's ISCM program): o The software should be detected and isolated/quarantined within the organization-defined timeframe. o The details regarding the platform affected and duration of software execution prior to remediation should be recorded At level 5, determine whether the agency has deployed automation that can identify in near-real time, the software deployed across the organization as well as the status of associated licenses, and other information needed for tracking purposes. For sampled systems, determine whether the information tracked is complete and accurate. The organization utilizes automation to update, in near real-time, the status of software licenses to ensure that the organization is not paying for unnecessary licenses or using unauthorized licenses. At level 5, IG evaluators should obtain evidence [ex. network scanning reports designed to identify all instances of software (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. IG evaluators should also obtain evidence (ex. EA documentation updates) that indicates that changes to the SW inventory (due to SW deployment and decommissioning) is reflected in the organization's enterprise architecture.

IG Metric - FY19	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
4. To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets (NIST SP 800-53 Rev. 4: RA-2, PM-7, and PM-	**Ad Hoc** The organization has not categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets.		At level 2, evaluate agency information security policies and procedures to determine if they define how the organization categories and communicates the importance and priority of its information systems. Furthermore, IG evaluators should determine whether the agency's policies and procedures in this area incorporate HVA related considerations, such as how HVA's are identified, prioritized, and secured. Furthermore, IG evaluators should determine whether the agency's information security policies, procedures, and/or control baselines have been updated to incorporate HVA considerations. For example, evaluate POA&M policies and procedures to determine whether HVA requirements have been established to determine if POA&M items are prioritized or validated/reviewed on a more frequent basis than non-HVAs. Evaluate ISCM policies and procedures to determine if HVAs are subject to more rigorous review processes. Furthermore, IG evaluators should analyze the agency's information security policies/procedures to determine how system classifications consider
	Defined The organization has categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets.	• Information classification standard and related policies and procedures • System/Information impact classification worksheets • Policy on categorization of information systems • Data dictionaries	
	Consistently Implemented The organization's defined importance/priority levels for its information systems considers risks from the supporting business functions and mission impacts, including for high value assets, and is used to guide risk management decisions.	• Security risk documentation (i.e., SSPs, categorization documents, HVA documents, system-level categorization sheets, etc.) • Approved organization-wide information systems inventory • Identification of mission essential systems and high value assets (HVAs)	
	Managed and Measurable The organization ensures the risk-based allocation of resources for the protection of high value assets through collaboration and data-driven prioritization.	•Business impact analysis	
	Optimized The organization utilizes impact-level prioritization for additional granularity to support risk-based decision-making.	• Cybersecurity Framework profiles	

IG Metric - FY19	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
5. To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy, including for supply chain risk management. This includes the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk (NIST SP 800-39; NIST SP 800-53 Rev. 4: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; OMB M-16-17; Green Book (Principle #6); CFO Council ERM Playbook; OMB M-17-25; NIST SP 800-37 (Rev. 2); NIST SP 800-161: Appendix E; CSF: ID.SC-1 – 2; SECURE Technology Act: s. 1326)?	**Ad Hoc** Risk management policies, procedures, and strategy have not been fully defined, established, and communicated across the organization. The organization has not performed an organization-wide assessment of security and privacy risks to serve as an input to its risk management policies, procedures, and strategy.	• Information security risk management standard and related procedures • Enterprise risk management policy and related procedures • Charters for committees involved with risk management • Enterprise risk management strategy • Agency communications or policies related to IT governance • Mission/business objectives •System-level security and privacy risk assessment results •Supply chain risk assessment results •Previous organization level security and privacy risk assessment results •Information sharing agreements and/or MOUs •Security and privacy information from ISCM activities	In assessing their organization(s) processes for conducting security and privacy risk assessments, IG evaluators should note that NIST 800-37, Rev. 2 states that guidance on privacy assessment reports and privacy management and reporting tools will be addressed in future publications. SP 800-37, Rev. 2 references NIST IR 8062 for guidance on conducting privacy risk assessments. At level 2, the organization should demonstrate that it has established the overall context within which the organization functions and includes consideration of factors that affect the ability of an agency to meet its stated mission and objectives. The CFO Council ERM playbook gives examples of the components that should be considered in understanding and defining the overall context, including goals and objectives, risk tolerance and appetite, and the availability and quality of information. Further, in accordance with Task P-2 in 800-137, Rev 2., at level 2, the organization should have established a risk management strategy that includes a determination of risk tolerance, acceptable risk assessment methodologies and risk response strategies, a process for consistently evaluating security and privacy risks organization-wide, and approaches for monitoring risk over time. The organization wide risk management strategy should guide and inform risk-based decisions including how security and privacy risk is framed, assessed, responded to, and monitored. At level 2, IG evaluators should obtain evidence that the organization is aggregating information from system level risk and privacy assessments and continuous monitoring efforts to assess information system and privacy risk at the organizational level (organization-wide assessment of security and privacy risks). Such evidence may include a risk profile, risk registers, dashboards, and program-level POA&Ms. As evidence of the performance of an organization-wide security and privacy risk assessment, determine whether the process to create the agency's risk profile included information security and privacy related risks. At level 2, the organization should prioritize its overall risks based on likelihood and impact and use the highest ranked risks to create the risk profile. At level 2, determine whether the organization's risk profile addresses (1) identification of objectives, (2) identification of risk, (3) inherent risk assessment, (4) current risk response, (5) residual risk assessment, (6) proposed risk response, and (7) proposed action category. Further, determine whether the enterprise level risk profile is consistently used for risk management activities at the business process and system levels. At level 2, IG evaluators should obtain organizational policies, procedures, and strategies that address how the organization has established its organizational risk management approach, methodologies and processes and communicated these policies, procedures, and strategies to all appropriate organizational, mission, and business owners. The policies/procedures/strategy should, at minimum, address the following:
	Defined The organization has performed an organization-wide security and privacy risk assessment. Risk management policies, procedures, and strategy have been developed and communicated across the organization. The strategy clearly states risk management objectives in specific and measurable terms. As appropriate, the organization has developed an action plan and outlined its processes to address the supply chain risk management strategy and related policy and procedural requirements of the SECURE Technology Act.		
	Consistently Implemented The organization consistently implements its risk management policies, procedures, and strategy at the enterprise, business process, and information system levels. The organization uses its risk profile to facilitate a determination of the aggregate level and types of risk that management is willing to assume. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of risk management processes and activities to update the program. In accordance with the SECURE Technology Act, the organization is taking measurable steps to implement its action plan for supply chain risk management.	•Enterprise level risk profile which identifies risks arising from mission and mission support operations •Enterprise risk management policy and related procedures •Action plan(s) for implementing the Security Technology Act	

IG Metric - FY19	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
5. (continued) To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy, including for supply chain risk management. This includes the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk (NIST SP 800-39; NIST SP 800-53 Rev. 4: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; OMB M-16-17; Green Book (Principle #6); CFO Council ERM Playbook; OMB M-17-25; NIST SP 800-	**<u>Managed and Measurable</u>** The organization monitors and analyzes its defined qualitative and quantitative performance measures on the effectiveness of its risk management strategy across disciplines and collects, analyzes and reports information on the effectiveness of its risk management program. Data supporting risk management metrics are obtained accurately, consistently, and in a reproducible format.	• Risk register/ERM reports and screenshots • Meeting minutes/lessons learned of committees involved in risk management	At level 3, for sampled systems and at the program level, determine whether information security and privacy risks are framed, assessed, responded to, and monitored (testing for Q#9 should serve as an input to this) in accordance with the organization's risk management strategy and supporting policies and procedures. At level 3, 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 that these can be used to determine if the organization has implemented security commensurate with the risk to the organization's mission and operations. (Is the organization operating within its defined risk appetite/tolerances?) (NIST SP 800-39, section 2.1). At level 3, IG evaluators should obtain the organization's risk profile and ensure that it contains the following information: 1. Identification of Objectives, 2. Identification of Risk, 3. Inherent Risk Assessment, 4. Current Risk Response, 5. Residual Risk Assessment, 6. Proposed Risk Response, and 7. Proposed Action Category (OMB Circular A-123) At level 3, IG evaluators should obtain the organization's risk management documentation (System Security Plans, Security Assessment Reports, System Risk Assessments, POAMs, etc.), and ensure the organization's systems are operating within the defined risk tolerances (i.e. the risk assumed/accepted is within defined aggregate level of risk acceptable and no unacceptable types of risk are assumed, as defined in the organization's risk profile) or the organization has documented POA&Ms to reduce the risk to be within the organization's defined risk appetite/tolerance (NIST SP 800-39, task 1-3 and H.1). At level 3, IG evaluators should obtain the lessons learned developed as a result of an assessment of the effectiveness of the organization's risk management processes, and evidence that this information was shared with organizationally-defined personnel.
	<u>Optimized</u> The enterprise risk management program is fully integrated with other security areas, such as ISCM, and other business processes, such as strategic planning and capital planning and investment control. Further, the organization's risk management program is embedded into daily decision making across the organization and provides for continuous risk identification.	• Investment/staffing documentation updates • Strategic planning documentation updates • Updates to the security program documentation (such as updates to ISCM documentation) • Updates to security performance metrics (and system security plans/Business Impact Assessment/COOP updates, etc.) based on ERM meetings/communications	

IG Metric - FY19	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
6. To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2); OMB M-19-03; FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA	**Ad Hoc** The organization has not defined an information security architecture and its processes for ensuring that new/acquired hardware/software are consistent with its security architecture prior to introducing systems into its development environment.		At level 2, verify that the organization has developed an organization-wide information security architecture. Ensure that development/maintenance of the information security architecture is coordinated with the Senior Agency Official for Privacy to ensure that security controls needed to support privacy requirements are identified and effectively implemented. Analyze the information security architecture to determine whether it describes the structure and behavior of the organization's security processes, information security systems, personnel, and organizational sub-units, showing their alignment with the organization's mission and strategic plans. Further, analyze the organization's system's development life cycle policies and procedures to determine whether the organization has defined system security engineering activities and tasks, as appropriate and in accordance with NIST 800-160v1. NIST 800-160v1 provides for flexibility on implementation of system security engineering principles and the intent at Level 2 is for IG evaluators to determine whether the organization, based on its missions, risks, and threats has integrated systems security engineering activities into its SDLC policies and procedures. At level 2, IG evaluators should obtain organizational policies, procedures and strategies that address how the organization has established its information security architecture and integrated its security
	Defined The organization has defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture. In addition, the organization has defined how it implements system security engineering principles within its system development life cycle.	• Related policies and procedures (including Architecture Review Board Charters) • System development methodology • Open source software policy • IT architecture policy • Desktop software approval procedures • Enterprise Architecture policies • Enterprise Architecture as-is and to-be states	
	Consistently Implemented The organization has consistently implemented its security architecture across the enterprise, business process, and system levels. System security engineering principles are followed and include assessing the impacts to the organizations information security architecture prior to introducing information system changes into the organization's environment.	• Sample Security architecture/SIAs reviews of new acquired hardware/software	
	Managed and Measurable The organization's information security architecture is integrated with its systems development lifecycle and defines and directs implementation of security methods, mechanisms, and capabilities to both the Information and Communications Technology (ICT) supply chain and the organization's information systems.	• Sample security/enterprise architecture status reports • Current vs future state enterprise architecture documents (highlighting the architecture changes resulting from hardware/software implementations)	
	Optimized The organization uses advanced technologies and techniques for managing supply chain risks. To the extent practicable, the organization is able to quickly adapt its information security and enterprise architectures to mitigate supply chain risks.	• Evidence of avoidance of the purchase of custom configurations • Evidence of the use of a diverse set of suppliers • Evidence of the use of approved vendor list with standing industry reputations	

IG Metric - FY19	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
6. (Continued) To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2); OMB M-19-03; FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?			At level 4, determine whether the information security architecture is incorporated into and aligned with the organization's system's development lifecycle and enterprise architecture processes. Furthermore, at Level 4, the information security architecture should provide for traceability from the highest level strategic goals and objectives of the organization (tier 1), through specific mission/business protection needs (tier 2), to specific information security solutions provided by people, processes, and technologies (tier 3). In addition, at level 4, the organization has the ability to validate (though continuous monitoring processes) that its system security engineering and system life cycle processes are being effectively implemented across the agency and that deviations are identified and managed. Testing results for Q's #2, #3, and the questions from the Detect-ISCM function area should be used to support maturity conclusions. For level 5, NIST SP 800-161 and NIST SP 800-53 provide examples of what is considered "advanced technologies and techniques for supply chain protection." Further, the organization implements supplier diversity concepts to ensure that [organization defined security safeguards] are obtained from different suppliers. An example could be the use of various suppliers for vulnerability scanning/configuration management at various stacks/levels (e.g., application, database, network/os).

IG Metric - FY19	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
7. To what degree have roles and responsibilities of internal and external stakeholders involved in risk management processes been defined and communicated	**Ad Hoc** Roles and responsibilities have not been defined and communicated across the organization.		At level 2, the organization's risk management policies/strategy should have clearly defined roles, responsibilities, delegated authorities, and accountability for individuals/committees that are part of the agency's ERM processes, including at the enterprise, business/mission, and system levels. The Institute of Internal Auditors Research Foundation notes that "in an effective organizational governance framework, roles, responsibilities, and accountabilities are defined" and "the assignment of authority, responsibility, and accountability must be documented and communicated to all personnel. OMB A-123 notes that agencies may use a Risk Management Council (RMC) to oversee the establishment of the agency's risk profile
	Defined Roles and responsibilities of stakeholders have been defined and communicated across the organization.	• Information security program policy and procedures • Enterprise risk management policy and procedures and strategy • Organizational chart outlining all agency offices/lines of business • Agency Strategic Plan (to identify agency mission, programs, projects, etc.) • Position descriptions	
	Consistently Implemented Individuals are performing the roles and responsibilities that have been defined across the organization.	• Budget documents for business units involved in risk management • Risk management committee charters and meeting minutes	
	Managed and Measurable Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement risk management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively. Additionally, the organization utilizes an integrated risk management governance structure for implementing and overseeing an enterprise risk management (ERM) capability that manages risks from information security, strategic planning and strategic reviews, internal control activities, and applicable mission/business areas.	• Charters/Meeting minutes for enterprise risk management committees • Organization-wide risk register • Enterprise risk profile	
	Optimized The organization's risk management program addresses the full spectrum of an agency's risk portfolio across all organizational (major units, offices, and lines of business) and business (agency mission, programs, projects, etc.) aspects.	• Evidence that the agency's risk profile, risk register, and risk management committee are addressing the full spectrum of agency risks • Evidence that risk management decisions are flowing through all three tiers of risk management (organizational, mission/business unit, and information system levels)	

IG Metric - FY19	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
8. To what extent has the organization ensured that plans of action and milestones (POA&Ms) are utilized for effectively mitigating security weaknesses (NIST SP 800-53 Rev. 4: CA-5; NIST SP 800-37 (Rev. 2);	**Ad Hoc** Policies and procedures for the effective use of POA&Ms to mitigate security weaknesses have not been defined and communicated.		At level 3, for sampled systems, verify that system level POA&M's describe the actions planned to correct deficiencies identified during security controls assessments and continuous monitoring activities (See 800-37, Rev 2, Task A-6, "Discussion"). The POA&M should include tasks to be accomplished to mitigate deficiencies, resources required to accomplish the tasks, milestones established to meet the tasks, and the scheduled completion dates for the milestones and tasks (See 800-37, Rev 2, Task A-6, "Discussion"). As noted in SP 800-37, Rev. 2, Task A-6, resources can include personnel, new hardware or software, and tools.
	Defined Policies and procedures for the effective use of POA&Ms have been defined and communicated. These policies and procedures address, at a minimum, the centralized tracking of security weaknesses, prioritization of remediation efforts, maintenance, and independent validation of POA&M activities.	• POA&M Guidance standard and related policies and procedures/ISCM policy/procedures/strategies • Continuous monitoring standard	
	Consistently Implemented The organization consistently implements POA&Ms, in accordance with the organization's policies and procedures, to effectively mitigate security weaknesses.	• System level POA&Ms (last 4 quarters) • POA&M validation reports • Sample system ATO's and continuous monitoring reports • Sample vulnerability scans for systems • Results of internal reviews • Enterprise wide POA&M	
	Managed and Measurable The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its POA&M activities and uses that information to make appropriate adjustments, as needed, to ensure that its risk posture is maintained.	• Evidence of tracking the effectiveness of risk response actions for risk reduction	
	Optimized The organization employs automation to correlate security weaknesses amongst information systems and identify enterprise-wide trends and solutions on a near real- time basis. Furthermore, processes are in place to identify and manage emerging risks, in addition to known security weaknesses.	• Evidence of POA&M automation (such as the use of a dashboard to view and correlate risks across the agency)	

IG Metric - FY19	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
9. To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system level risk assessments, including for identifying and prioritizing (i) internal and	**Ad Hoc** Policies and procedures for system level risk assessments and security control selections have not been defined and communicated.		At level 2, the organization should specify in its policies and procedures how system level risk assessments (tier 3) are conducted, documented, reviewed, disseminated, and updated. At level 2, the organization's policy/procedures should clearly stipulate controls that are system-level, program-level, hybrid, and common to facilitate risk assessments. Furthermore, as noted in NIST 800-30, organizations also provide guidance on how to identify reasons for uncertainty when risk factors are assessed and how to compensate for incomplete, imperfect, or assumption-dependent estimates. The organization's policies/procedures should also provide guidance on what level of risks (combination of likelihood and impact) indicate that no further analysis of any risk factors is needed. As noted in NIST 800-37, Rev 2, Task P-14, organizations determine the form of risk assessment conducted for information
	Defined Policies and procedures for system level risk assessments and security control selections are defined and communicated. In addition, the organization has developed a tailored set of baseline criteria that provides guidance regarding acceptable risk assessment approaches and controls to be evaluated tailored to organizational and system risk.	• System level risk/security assessment policies and procedures • Continuous monitoring standard	
	Consistently Implemented System risk assessments are performed and appropriate security controls 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.	• Organization's tailored set of baseline security controls • Risk/security assessment for sampled systems • Risk tolerance levels • Vulnerability scan results	
	Managed and Measurable The organization consistently monitors the effectiveness of risk responses to ensure that enterprise-wide risk tolerance is maintained at an appropriate level.	• Periodic reviews of risk tolerance levels • ISCM Strategy • Continuous monitoring reports/dashboards • ERM meeting minutes	
	Optimized The organization utilizes Cybersecurity Framework profiles to align cybersecurity outcomes with mission or business requirements, risk tolerance, and resources of the organization.		

IG Metric - FY19	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
10. To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders (CFO Council ERM Playbook; OMB A-123; OMB Circular A-11; Green Book (Principles	**Ad Hoc** The organization has not defined how information about risks are communicated in a timely manner to all necessary internal and external stakeholders.		At Level 2, as noted in the Green Book, 13.02, the agency has designed a process that uses the organization's and related risks to identify the information requirements needed to achieve the objectives and address risks. Information requirements consider the expectations of both internal and external users at each tier (organizational, business process, and system level). Management defines the identified information requirements at the appropriate level and requisite specificity for appropriate personnel. As such, at Level 2, the organization's risk management policies/procedures/strategy, should identify the information requirements for risk communication for the various tiers (enterprise, business process, and system level) as well as for the key internal and external stakeholders defined in Question #7.
	Defined The organization has defined how information about risks are communicated in a timely manner to all necessary internal and external stakeholders.	• Risk management policies and procedures	
	Consistently Implemented The organization ensures that information about risks is communicated in a timely and consistent manner to all internal and external stakeholders with a need-to-know. Furthermore, the organization actively shares information with partners to ensure that accurate, current information is being distributed and consumed.	• Sample of Risk Management documentation (ex. SSP/RAs, SARs, etc.) • Internal communications to stakeholders about risk (ex. emails, meeting minutes, etc.) • Sample system level POA&M's • Enterprise-wide POA&M	
	Managed and Measurable The organization employs robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of interrelated risks across the organization. The dashboard presents qualitative and quantitative metrics that provide indicators of risk.	• Continuous monitoring reports • Risk register • Vulnerability management dashboards • CDM and SIEM outputs/alerts/reports • Continuous monitoring dashboards	
	Optimized Through the use of risk profiles and dynamic reporting mechanisms, the risk management program provides a fully integrated, prioritized, enterprise-wide view of organizational risks to drive strategy and business decisions.	• Enterprise risk profile • Enterprise-wide and component-level risk management dashboards • investment/staffing documentation • Updates to ERM program • Target-state enterprise architecture documentation updates	

IG Metric - FY19	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
11. To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services (NIST SP 800-53 REV. 4: SA-4; NIST SP 800-152; NIST SP 800-37 Rev.	**Ad Hoc** The organization has not defined a process that includes information security and other business areas as appropriate for ensuring that contracts and other agreements for contractor systems and services include appropriate clauses to monitor the risks related to such systems and services. Further, the organization has not defined its processes for ensuring appropriate information security oversight of contractor provided systems and services.		Consider how supply chain risk management, referred to in Question #6, is addressed through the procurement process. For level 2, IG evaluators should evaluate the agency's procurement and information security policies/procedures, as appropriate, to determine if they provide requirements and a process for ensuring that acquisitions for information system, system component, and/or related services (including cloud-based) include security functional requirements, security strength requirements, security assurance requirements, security-related documentation requirements, and acceptance criteria (NIST SP 800-53, Rev. 4, SA-4). Furthermore, IG evaluators should determine whether the agency's procurement policies define specific information security clauses/requirements for contracts where agency data is processed, stored, and/or transmitted to a supplier/vendor (including for cloud-based systems). For level 2, IG evaluators should determine whether the agency's procurement and information security policies/procedures, as appropriate, define and document government oversight and user roles and responsibilities with respect to third party oversight (including for cloud service providers). The policies and procedures should stipulate the organization's processes to ensure that security controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and
	Defined The organization has defined a process that includes information security and other business areas as appropriate for ensuring that contracts and other agreements for third party systems and services include appropriate clauses to monitor the risks related to such systems and services. In addition, the organization has defined its processes to ensure that security 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.	• Procurement policies (which include coordination with IT to ensure all requisite information is included in IT services) • Standard contracting language/templates • Third party assurance requirements and standards	
	Consistently Implemented The organization ensures that specific contracting language and SLAs are consistently included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services. Further, the organization obtains sufficient assurance, through audits, test results, or other forms of evaluation, that the security 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.	• Third party security questionnaires • Contracts, task orders, statements of work for sample IT service providers • Sample Service level agreements • Sample Terms of service agreements • Sample Continuous monitoring reports for third party providers	
	Managed and Measurable The organization uses qualitative and quantitative performance metrics (e.g., those defined within SLAs) to measure, report on, and monitor information security performance of contractor-operated systems and services.	• Contractor performance reports (or similar monitoring)	
	Optimized The organization analyzes the impact of material changes to security assurance requirements on its vendor relationships and ensures that contract vehicles are updated as soon as possible.		

IG Metric - FY19	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
12. To what extent does the organization utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; CFO Council ERM Playbook)?	**Ad Hoc** The organization has not identified and defined its requirements for an automated solution to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependences, risk scores/levels, and management dashboards.		At level 3, the organization should demonstrate that it has implemented technology to provide insight into all areas of organizational exposure to risk (such as reputational, programmatic, performance, financial, IT, acquisitions, human capital, etc.). The objective is to deploy technology that enables an enterprise wide view of risks across the organization and related control and remediation activities. In addition, at level 3, the organization should demonstrate that it is using/providing information to the Federal dashboard as part of DHS' CDM program, as appropriate. At level 4, the organization utilizes cyber threat modeling to inform efforts related to cybersecurity and resilience. Specifically, the organization utilizes cyber threat modeling as a component of cyber risk framing, analysis and assessment, and evaluation of alternative responses (individually or in the context of cybersecurity portfolio management). As part of this effort, the organization has selected a cyber threat modeling framework. For additional information, refer to *Cyber Threat Modeling: Survey, Assessment, and Representative Framework* , April 7, 2018. Available at https://www.mitre.org/sites/default/files/publications/pr_18-1174-ngci-cyber-threat-modeling.pdf . At level 4, the organization can demonstrate the effect that a potential threat exploiting a vulnerability would cause to the organization and incorporates this information into its risk responses. IG evaluators should
	Defined The organization has identified and defined its requirements for an automated solution that provides a centralized, enterprise wide view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards.	• Risk Management/ISCM policies/procedures/strategies/requirements document for GRC tool • SOPs for GRC tool	
	Consistently Implemented The organization consistently implements an automated solution across the enterprise that provides a centralized, enterprise wide view of risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. All necessary sources of risk information are integrated into the solution.	• Risk register screenshots • FISMA compliance tool dashboard screenshots • GRC-generated ISCM 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.	• Evidence of scenario analyses/response modeling for potential threats	
	Optimized The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its risk management program.	• Evidence of benchmarking and making improvements to the ERM program • CDM and SIEM outputs (that include alerts/reports derived from correlating information from technologies designed to identify vulnerabilities, baseline-configuration compliance, APTs, etc.) to regularly analyze performance against the organization-defined benchmarks/performance metrics to ensure that the risk management program continues to improve	
13. Provide any additional information on the effectiveness (positive or negative) of the organization's risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?	N/A	N/A	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
14. To what degree have the roles and responsibilities of configuration management stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: CM-1; NIST SP 800-128: Section 2.4)?	**Ad Hoc** Roles and responsibilities at the organizational and information system levels for stakeholders involved in information system configuration management have not been fully defined and communicated across the organization.		At level 2, consider whether roles and responsibilities have been defined, including for developing and maintaining metrics on the effectiveness of information system configuration management activities. At level 3, interview staff and management responsible for configuration management and change control activities to determine whether adequate resources have been provisioned.
	Defined Roles and responsibilities at the organizational and information system levels for stakeholders involved in information system configuration management have been fully defined and communicated across the organization. Staff are assigned responsibilities for developing and maintaining metrics on the effectiveness of information system configuration management activities.	• Enterprise-Wide Configuration Management Plan • Configuration Control Board Charter • Organizational charts • Information Security Program policies and related procedures to facilitate the implementation of CM polices and controls	
	Consistently Implemented Individuals are performing the roles and responsibilities that have been defined across the organization.	• Evidence of budgeting for tools and appropriate staffing levels	
	Managed and Measurable Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively perform information system configuration management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.		

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
15. To what extent does the organization utilize an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or	**Ad Hoc** The organization has not developed an organization wide configuration management plan with the necessary components.		For level 3, for sampled systems, select a sample of configuration changes for which the organization's configuration management and/or change control processes would apply. For these sample changes, determine whether the appropriate risk assessment activities were performed. For level 5, based on the results of analysis performed for Questions 17 and 18 below, determine whether the configuration
	Defined The organization has developed an organization wide configuration management plan that includes the necessary components.	• Enterprise-Wide Configuration Management Plan • Configuration Control Board Charter	
	Consistently Implemented The organization has consistently implemented an organization wide configuration management plan and has integrated its plan with its risk management and continuous monitoring programs. Further, the organization utilizes lessons learned in implementation to make improvements to its plan.	• Sample of configuration change requests for review/analysis, approval, notifications of change, implementation, and closure documentation • Evidence of lessons learned being performed for Configuration Management activities with associated updates to CM plan	
	Managed and Measurable The organization monitors, analyzes, and reports to stakeholders qualitative and quantitative performance measures on the effectiveness of its configuration management plan, uses this information to take corrective actions when necessary, and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.	• Configuration Management testing documentation • Evidence of tracking configuration management metrics (as outlined in Configuration Management plan)	
	Optimized The organization utilizes automation to adapt its configuration management plan and related processes and activities to a changing cybersecurity landscape on a near real-time basis (as defined by the organization).	• See additional guidance provided	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
16. To what degree have information system configuration management policies and procedures been defined and implemented across the organization? (Note: the maturity level should take into consideration the maturity of questions 17, 18, 19, and 21) (NIST SP 800-53 REV.4: CM-1	**Ad Hoc** The organization has not developed, documented, and disseminated comprehensive policies and procedures for information system configuration management.		Based on the results of analysis performed for Questions 17 and 18 below, determine whether the configuration management plan is being updated in a near-real time basis.
	Defined The organization has developed, documented, and disseminated comprehensive policies and procedures for managing the configurations of its information systems. Policies and procedures have been tailored to the organization's environment and include specific requirements.	• System-level Configuration Management policies and procedures • System-level Security Plans • Organization-wide information security policy • Enterprise-wide configuration management plan • Hardening guides	
	Consistently Implemented The organization consistently implements its policies and procedures for managing the configurations of its information systems. Further, the organization utilizes lessons learned in implementation to make improvements to its policies and procedures.	• Testing (e.g., through vulnerability scanning) of configuration changes/baselines/settings for a sample of systems • Evidence of lessons learned being performed to improve policy and procedures	
	Managed and Measurable The organization monitors, analyzes, and reports on the qualitative and quantitative performance measures on the effectiveness of its configuration management policies and procedures and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.	• Information Security Continuous Monitoring (ISCM) Strategy/Continuous Monitoring reports • Analysis of vulnerability scanning and remediation activities for a sample of systems • Evidence of tracking configuration management metrics (as outlined in configuration management plan)	
	Optimized On a near real-time basis, the organization actively adapts its configuration management plan and related processes and activities to a changing cybersecurity landscape to respond to evolving and sophisticated threats.	• See additional guidance provided	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
17. To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53 REV. 4: CM-2 and CM-8; FY 2019 CIO FISMA Metrics: 1.1, 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1)?	**Ad Hoc** The organization has not established policies and procedures to ensure that baseline configurations for its information systems are developed, documented, and maintained under configuration control and that system components are inventoried at a level of granularity deemed necessary for tracking and reporting.		At level 3, IG evaluators should verify for sampled systems that organization implements secure images or templates based on the organization's approved configuration standards. Observe evidence of tie-in and real-time use of system inventory, Configuration Management Database (CMDB) or related tools, and Asset Baseline monitoring tools. At level 4, IG evaluators should verify that the organization employs automation to maintain consistent configuration baseline information, For example, for sampled systems, IG evaluators should verify that system inventory tools, have been deployed
	Defined The organization has developed, documented, and disseminated its baseline configuration and component inventory policies and procedures.	• Configuration Management policy/procedures for establishing baselines • Asset Inventory policy and procedures (information should be found in the Configuration Management Plan) • Baseline Configurations (System-level security plans)	
	Consistently Implemented The organization consistently records, implements, and maintains under configuration control, baseline configurations of its information systems and an inventory of related components in accordance with the organization's policies and procedures.	• For select sample systems, obtain evidence of maintenance of baseline information	
	Managed and Measurable The organization employs automated mechanisms (such as application whitelisting and network management tools) to detect unauthorized hardware, software, and firmware on its network and take immediate actions to limit any security impact.	• Evidence of a use of Asset Baseline monitoring tool(s) • Host-based Intrusion Prevention System (HIPS) policies • Continuous Diagnostics and Mitigation (CDM) dashboards • Observation and data analysis of information in network management tools • Automated mechanisms to detect presence of unauthorized hardware, software, and firmware components (including remote and mobile)	
	Optimized The organization utilizes technology to implement a centralized baseline configuration and information system component inventory process that includes information from all organization systems (hardware and software) and is updated in a near real-time basis.	• Evidence of a Configuration Management Database (CMDB) or related tool that includes baselines with historical retention for roll back	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
18. To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53 REV. 4: CM-6, CM-7, and SI-2; FY 2019 CIO FISMA Metrics: 1.1 and 2.2; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?	**Ad Hoc** The organization has not established policies and procedures for ensuring that configuration settings/common secure configurations are defined, implemented, and monitored.		At level 2, 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 (See CIGIE web application report). 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).
	Defined The organization has developed, documented, and disseminated its policies and procedures in this area and developed 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 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.	• 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	
	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.	• Dashboards that highlight in real-time the devices on the network and their compliance with the agency's baselines	
	Optimized The organization deploys system configuration management tools that automatically enforce and redeploy configuration settings to systems at frequent intervals as defined by the organization, or on an event driven basis.	• Evidence of frequent, enforced system configurations • Evidence of event-triggered configuration, Automated configuration from Continuous Diagnostics and Mitigation (CDM) events • Automated routing/approval process and queues to enforce process and prevent out-of-sequence events	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
19. To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53 REV. 4: CM-3 and SI-2; NIST SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20,	**Ad Hoc** The organization has not developed, documented, and disseminated its policies and procedures for flaw remediation.		For a sample of systems, obtain and analyze evidence of the remediation of configuration-related vulnerabilities within established timeframes.
	Defined The organization has developed, documented, and disseminated its policies and procedures for flaw remediation. 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. In addition, the organization patches critical vulnerabilities within 30 days.	• 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	
	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.	• Evidence of automated flaw remediation using trusted, verified repositories for operating systems • Metrics to measure (turnaround) performance and make continuous improvements • 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, as appropriate, where such tools are available and safe.	• 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	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
20. To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-08-05)?	**Ad Hoc** The organization has not prepared and planned to meet the goals of the TIC initiative. This includes plans for reducing and consolidating its external connections, routing agency traffic through defined access points, and meeting the critical TIC security controls.		
	Defined The organization has defined its plans for meeting the goals of the TIC initiative and its processes for inventorying its external connections, meeting the defined TIC security controls, and routing all agency traffic through defined access points. Further the agency has identified the TIC 2.0 capabilities enabled by its provider, the critical capabilities that it manages internally, and the recommended capabilities that are provided through the TIC provider or internally.	• Organization's TIC plan • Contract/SOW/Task Order with MTIPS provider • Inventory of external connections	
	Consistently Implemented The organization has consistently implemented its TIC approved connections and critical capabilities that it manages internally. The organization has consistently implemented defined TIC security controls, as appropriate, and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate.	• Network Diagram • TIC Capability Scores • TIC Reference Architecture • Einstein alerts	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
21. To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions;	**Ad Hoc** The organization has not developed, documented, and disseminated its policies and procedures for managing configuration change control. Policies and procedures do not address, at a minimum, one or more of the necessary configuration change control related activities.		Evaluate the agency's processes for ensuring that all web application changes are appropriately authorized (See CIGIE Web Application Report for additional details).
	Defined The organization has developed, documented, and disseminated its policies and procedures for managing configuration change control. The policies and procedures address, at a minimum, the necessary configuration change control related activities.	• Change control policies and procedures • CCB Charter	
	Consistently Implemented The organization consistently implements its change control policies, procedures, and processes, including explicitly consideration of security impacts prior to implementing changes.	• Sample of change control tickets for systems • Testing and Security Impact Analyses	
	Managed and Measurable The organization monitors, analyzes, and reports on the qualitative and quantitative performance measures on the effectiveness of its change control activities and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.	• Evidence of monitoring, analyzing, and reporting on Configuration Management metrics (as outlined in Configuration Management plan)	
22. Provide any additional information on the effectiveness (positive or negative) of the organization's configuration management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?	N/A	N/A	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
23. To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV 4: AC-1, IA-1, and PS-1; Federal Identity, Credential, and Access	**Ad Hoc** Roles and responsibilities at the organizational and information system levels for stakeholders involved in ICAM have not been fully defined and communicated across the organization.		To determine whether adequate resources have been dedicated to this program, interview relevant stakeholders and evaluate budget requests. For level 2, consider whether roles and responsibilities include those for developing and maintaining metrics on the
	Defined Roles and responsibilities at the organizational and information system levels for stakeholders involved in ICAM have been fully defined and communicated across the organization. This includes, as appropriate, developing an ICAM governance structure to align and consolidate the agency's ICAM investments, monitoring programs, and ensuring awareness and understanding. In addition, staff are assigned responsibilities for developing, managing, and monitoring metrics on the effectiveness of ICAM activities.	• Agency-wide information security policy, ICAM strategy, policies, and procedures • Business case for agency wide ICAM investments	
	Consistently Implemented Individuals are performing the roles and responsibilities that have been defined across the organization.	• Organizational charts • OMB ICAMC Federal Level Working Groups Meetings & distributed guidance	
	Managed and Measurable Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement identity, credential, and access management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.		

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
24. To what degree does the organization utilize an ICAM strategy to guide its ICAM processes and activities (FICAM)?	**Ad Hoc** The organization has not developed an ICAM strategy that includes a review of current practices ("as-is" assessment), identification of gaps (from a desired or "to-be state"), and a transition plan.		
	Defined The organization has defined its ICAM strategy and developed milestones for how it plans to align with Federal initiatives, including strong authentication, the FICAM segment architecture, and phase 2 of DHS's Continuous Diagnostics Mitigation (CDM) program, as appropriate.	• ICAM strategy and plans • ICAM architecture • Project plan for implementation of strong authentication and single sign-on, as appropriate • MOA (or similar document) with DHS for CDM program	
	Consistently Implemented The organization is consistently implementing its ICAM strategy and is on track to meet milestones.	• ICAM roadmap (or other document(s) that shows progress in meeting milestones)	
	Managed and Measurable The organization has transitioned to its desired or "to-be" ICAM architecture and integrates its ICAM strategy and activities with its enterprise architecture and the FICAM segment architecture.	• FICAM segment architecture • Enterprise architecture	
	Optimized On a near real-time basis, the organization actively adapts its ICAM strategy and related processes and activities to a changing cybersecurity landscape to respond to evolving and sophisticated threats.	• Lessons learned processes • Analysis of the timeliness of updates being made to ICAM policies and procedures relative to changing Federal requirements and guidance and the agency's risk environment	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
25. To what degree have ICAM policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 26 through 31) (NIST SP 800-	**Ad Hoc** The organization has not developed, documented, and disseminated its policies and procedures for ICAM.		
	Defined The organization has developed, documented, and disseminated its policies and procedures for ICAM. Policies and procedures have been tailored to the organization's environment and include specific requirements.	• ICAM strategy, policies, and procedures • Personnel security policies and procedures	
	Consistently Implemented The organization consistently implements its policies and procedures for ICAM, including for account management, separation of duties, least privilege, remote access management, identifier and authenticator management, and identification and authentication of non-organizational users. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its ICAM policies, procedures, and processes to update the program.	• Evidence of capturing and sharing lessons learned (i.e. meeting minutes, surveys, after-action reports, etc.) • Process for updating the program	
	Managed and Measurable The organization uses automated mechanisms (e.g. machine-based, or user based enforcement), where appropriate, to manage the effective implementation of its policies and procedures. Examples of automated mechanisms include network segmentation based on the label/classification of information stored on the servers; automatic removal/disabling of temporary/emergency/inactive accounts, use of automated tools to inventory and manage accounts and perform segregation of duties/least privilege reviews.	• Screenshots of automated mechanisms (i.e. network segmentation based on the label/classification of information stored on the servers; automatic removal/disabling of temporary/emergency/inactive accounts; automated tools to inventory and manage accounts and perform separation of duties/least privilege reviews)	
	Optimized The organization employs adaptive identification and authentication techniques to assess suspicious behavior and potential violations of its ICAM policies and procedures on a near-real time basis.	• Screenshots of proactive monitoring of user accounts • Examples of alerts sent for suspicious behavior/violations of ICAM policies	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
26. To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems (NIST SP 800-53 REV. 4: PS-2 and PS-3; National Insider Threat Policy; CSF: PR.IP-11)?	**Ad Hoc** The organization has not defined its processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems.		
	Defined The organization has defined its processes for ensuring that all personnel are assigned risk designations and appropriately screened prior to being granted access to its systems. Processes have been defined for assigning risk designations for all positions, establishing screening criteria for individuals filling those positions, authorizing access following screening completion, and rescreening individuals on a periodic basis.	• Personnel security policies and procedures • Screening criteria and procedures (if separate from personnel security policies) • Insider threat program strategy and policy	
	Consistently Implemented The organization ensures that all personnel are assigned risk designations, appropriately screened prior to being granted system access, and rescreened periodically.	• Background investigation and adjudication records for sampled users (privileged and non-privileged) • HR records showing assignment of risk designations for sampled positions	
	Managed and Measurable The organization employs automation to centrally document, track, and share risk designations and screening information with necessary parties, as appropriate.	• Screenshots/Observation of an automated tool or other automated mechanism to centrally manage and share risk designations and screening information	
	Optimized On a near-real time basis, the organization evaluates personnel security information from various sources, integrates this information with anomalous user behavior data (audit logging) and/or its insider threat activities, and adjusts permissions accordingly.	• User activity audit logs • Observation of a SIEM tool capturing this analysis and log review on a near real-time basis	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
27. To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained (NIST SP 800	**Ad Hoc** The organization has not defined its processes for developing, documenting, and maintaining access agreements for individuals that access its systems.		At level 4, the organization has mechanisms in place to automatically alert the appropriate individuals when access agreements need to be updated/reviewed.
	Defined The organization has defined its processes for developing, documenting, and maintaining access agreements for individuals.	• ICAM policies and procedures • Information security program policy • User access form/ROB/NDA templates • Acceptable use policy and method for acknowledgement	
	Consistently Implemented The organization ensures that access agreements for individuals are completed prior to access being granted to systems and are consistently maintained thereafter. The organization utilizes more specific/detailed agreements for privileged users or those with access to sensitive information, as appropriate.	• Sample of access agreements, rules of behavior, NDAs, for general and privileged users • Screenshots of system use notification for sample internal and external systems	
	Managed and Measurable The organization centrally manages user access agreements for privileged and non-privileged users.	• Screenshots of automated tool or observation of other centralized method to manage access agreements	
	Optimized On a near real-time basis, the organization ensures that access agreements for privileged and non-privileged users are updated, as necessary.	• Alerting function/automation that access agreements need to be refreshed in accordance with agency policy	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
28. To what extent has the organization implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.4 and 2.7; CSF: PR.AC-1 and 6; and Cybersecurity Sprint)?	**Ad Hoc** The organization has not planned for the use of strong authentication mechanisms for non-privileged users of the organization's facilities, systems, and networks, including for remote access. In addition, the organization has not performed e-authentication risk assessments to determine which systems require strong authentication.		Test (with a non-privileged user) login without PIV or LOA4 credential and see if access will still be authenticated. Analyze OS-level configuration settings to determine whether strong authentication is enabled and enforced. At level 5, sample select systems and test whether AD/PIV-based single sign on is enabled and enforced.
	Defined The organization has planned for the use of strong authentication mechanisms for non-privileged users of the organization's facilities, systems, and networks, including the completion of E-authentication risk assessments.	• Project plan for implementation of strong authentication • E-authentication risk assessment policy and procedures	
	Consistently Implemented The organization has consistently implemented strong authentication mechanisms for non- privileged users of the organization's facilities and networks, including for remote access, in accordance with Federal targets.	• E-authentication risk assessments for sample systems • System security plan for sampled systems • OS-level configuration settings related to strong authentication	
	Managed and Measurable All non-privileged users 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	
	Optimized The organization has implemented an enterprise-wide single sign on solution and all of the organization's systems interface with the solution, resulting in an ability to manage user (non-privileged) accounts and privileges centrally and report on effectiveness on a 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	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
29. To what extent has the organization implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; DHS ED 19-01; and	**Ad Hoc** The organization has not planned for the use of strong authentication mechanisms for privileged users of the organization's facilities, systems, and networks, including for remote access. In addition, the organization has not performed e-authentication risk assessments to determine which systems require strong authentication.		Test (with a privileged user) login without PIV or LOA4 credential and see if access will still be authenticated. Analyze OS-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.
	Defined The organization has planned for the use of strong authentication mechanisms for privileged users of the organization's facilities, systems, and networks, including the completion of E- authentication risk assessments.	• Project plan for implementation of strong authentication • E-authentication risk assessment policy and procedures	
	Consistently Implemented The organization has consistently implemented strong authentication mechanisms for privileged users of the organization's facilities and networks, including for remote access, in accordance with Federal targets.	• E-authentication risk assessments for sample systems • System security plan for sampled systems • OS-level configuration settings related to strong authentication	
	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	
	Optimized The organization has implemented an enterprise-wide single sign on solution and all of 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	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
30. 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	**Ad Hoc** The organization has not defined its processes for provisioning, managing, and reviewing privileged accounts.		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
	Defined The organization has defined its processes for provisioning, managing, and reviewing privileged accounts. Defined processes cover approval and tracking, inventorying and validating, and logging and reviewing privileged users' accounts.	• ICAM policies and procedures • Audit logging policies and procedures	
	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 operating system 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	
	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	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
31. To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53	**Ad Hoc** The organization has not defined the configuration/connection requirements for remote access connections, including use of FIPS 140-2 validated cryptographic modules, system time-outs, and monitoring and control of remote access sessions.		Evaluate the agency's ability to disconnect remote access sessions in a timely fashion based on potential malicious activity or abnormal behaviors on the network. Such activity could include unauthorized/large data transfers, etc.
	Defined The organization has defined its configuration/connection requirements for remote access connections, including use of cryptographic modules, system time-outs, and how it monitors and controls remote access sessions.	• Remote access policies and procedures • Audit logging policies and procedures	
	Consistently Implemented The organization ensures that FIPS 140-2 validated cryptographic modules are implemented for its remote access connection method(s), remote access sessions time out after 30 minutes (or less), and that remote users' activities are logged and reviewed based on risk.	• Configuration of VPN solution and settings for system timeouts and encryption • List of auditable events for remote access solution • Encryption cert for VPN server/browser settings • Log review report for remote access connections	
	Managed and Measurable The organization ensures that end user devices have been appropriately configured prior to allowing remote access and restricts the ability of individuals to transfer data accessed remotely to non-authorized devices.	• Configuration of DLP or other mechanism preventing transfer of data to non-authorized devices • Documentation of the checks performed on host systems prior to remote connection	
	Optimized The organization has deployed a capability to rapidly disconnect remote access user sessions based on active monitoring. The speed of disablement varies based on the criticality of missions/business functions.	• See additional guidance provided	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
32. Provide any additional information on the effectiveness (positive or negative) of the organization's identity and access management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?	N/A	N/A	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
33. To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems (NIST SP 800-122; NIST SP 800-37 (Rev. 2); OMB M-18-02; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J)?	**Ad Hoc** The organization has not established a privacy program and related plans, policies, and procedures as appropriate for the protection of PII collected, used, maintained, shared, and disposed of by information systems. Additionally, roles and responsibilities for the effective implementation of the organization's privacy program have not been defined		The inventory of PII referenced in this question refers to the types of PII collected for each system within the agency's system inventory. It is not meant to be an inventory of the PII data itself.
	Defined The organization has defined and communicated its privacy program plan and related policies and procedures for the protection of PII that is collected, used, maintained, shared, and disposed of by its information systems. In addition, roles and responsibilities for the effective implementation of the organization's privacy program have been defined and the organization has determined the resources and optimal governance structure needed to effectively implement its privacy program.	• Privacy program strategy/plan for implementing applicable privacy controls policies and procedures • Privacy policies and procedures related to protection of PII in information systems • Privacy program organizational chart, budget, reporting structure, roles and responsibilities, etc.	
	Consistently Implemented The organization consistently implements its privacy program by: • Dedicating appropriate resources to the program • Maintaining an inventory of the collection and use of PII • Conducting and maintaining privacy impact assessments and system of records notices for all applicable systems. • Reviewing and removing unnecessary PII collections on a regular basis (i.e., SSNs)	• PII Inventory (the types of PII records maintained by system and their sources) • PIAs and SORNs for a sample of systems • Sample of PII reviews • Staffing vacancies in the privacy program • Evidence of agency's plans to remove unnecessary PII	
	Managed and Measurable The organization monitors and analyses quantitative and qualitative performance measures on the effectiveness of its privacy activities and uses that information to make appropriate adjustments as needed.	• Performance measure reports/dashboards	
	Optimized The privacy program is fully integrated with other security areas, such as ISCM, and other business processes, such as strategic planning and risk management. Further, the organization's privacy program is embedded into daily decision making across the organization and provides for continuous identification of privacy risks. The organization conducts an independent review of its privacy program and makes adjustments as needed.	• ISCM strategy • Strategic plan • Risk management strategy • Report from independent review of the privacy program	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
34. 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? (NIST	**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 policy/data life cycle/protection policies and procedures • Data classification/handling 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.	• Screenshots/observation of database configuration settings related to encryption of data at rest for a sample of systems • Screenshots/observation of use of SSL/TLS (approved version) across external communication boundaries • Screenshots/observation/testing of network access controls or other methods used to prevent and detect untrusted removable media • Evidence of destruction/sanitization for a sample of devices	
	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 as long as 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 a sample of devices that contain sensitive information • Data dictionary for systems containing PII, highlighting the fields used to record PII collection • Evidence of data storage/destruction in accordance with the data retention schedule	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
35. To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53 REV. 4: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2019 CIO FISMA Metrics: 3.8;	**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.		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 such defenses related to USB and other removable media.
	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, audits its DNS records, and ensures the use of valid encryption certificates for its domains.	• Rules configured for DLP and other tools used to monitor outbound traffic, detect encrypted exfiltration, anomalous traffic patterns, and elements of PII	
	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.	• After-action reports/meeting minutes from exfiltration exercises	
	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	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
36. To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events? (NIST SP 800-122; NIST SP 800-53 REV. 4: Appendix J, SE-2; FY 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M-17-25)?	**Ad Hoc** The organization has not defined a Data Breach Response Plan that includes the agency’s policies and procedures for reporting, investigating, and managing a privacy-related breach. Further, the organization has not established a Breach Response team that includes the appropriate agency officials.		Evaluate whether the agency is prepared to identify individuals affected by a breach and is able to notify those individuals.
	Defined The organization has defined and communicated its Data Breach Response Plan, including its processes and procedures for data breach notification. Further, a Breach Response team has been established that includes the appropriate agency officials.	• Data Breach Response Plan • Roles and responsibilities of the breach response team(s)	
	Consistently Implemented The organization consistently implements its Data Breach Response plan. Additionally, the Breach Response team participates in table-top exercises and uses lessons learned to make improvements to the plan as appropriate. Further, the organization is able to identify the specific individuals affected by a breach, send notice to the affected individuals, and provide those individuals with credit monitoring and repair services, as necessary.	• Meeting minutes from breach response team meetings • Results of tabletop exercises • After action reports/lessons learned from tabletop exercises • MOU/A with credit monitoring/repair service	
	Managed and Measurable The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	• Evidence of use of metrics to measure effectiveness of Data Breach Response Plan	
	Optimized The organization's Data Breach Response plan is fully integrated with incident response, risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. Further the organization employs automation to monitor for potential privacy incidents and takes immediate action to mitigate the incident and provide protection to the affected individuals.	• Evidence showing integration with other security domains, including continuity of operations, ISCM, risk management, and incident response • Evidence of active monitoring of the DarkNet for potential privacy incidents	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
37. To what degree does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53 REV. 4: AR-5)? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out	**Ad Hoc** The organization has not defined its privacy awareness training program based on the organizational requirements, culture, and the types of PII that its users have access to. In addition, the organization has not developed role-based privacy training for individuals having responsibility for PII or activities involving PII.		
	Defined The organization has defined and communicated its privacy awareness training program, including role-based privacy awareness training and the training has been tailored to its mission and risk environment.	• Privacy program strategy/plan for implementing applicable privacy controls policies and procedures • Privacy policies and procedures related to protection of PII • Content of the privacy awareness training and role-based training	
	Consistently Implemented The organization ensures that all individuals receive basic privacy awareness training and individuals having responsibilities for PII or activities involving PII receive role-based privacy awareness training at least annually. Additionally, the organization ensures that individuals certify acceptance of responsibilities for privacy requirements at least annually.	• Records of completion of privacy awareness and role-based training • Evidence of certification of acceptance of responsibilities as part of the training (or separate process)	
	Managed and Measurable The organization measures the effectiveness of its privacy awareness training program by obtaining feedback on the content of the training and conducting targeted phishing exercises for those with responsibility for PII. Additionally, the organization make updates to its program based on statutory, regulatory, mission, program, business process, information system requirements, and/or results from compliance monitoring and auditing.	• Surveys (or other means) to gather feedback on the content of privacy training • Results of targeted phishing exercises • Content of the targeted phishing exercise • Evidence showing a reduction of privacy-related incidents due to employee negligence or human error • Evidence showing updates made to the privacy program as a result of the training feedback and exercises	
	Optimized The organization has institutionalized a process of continuous improvement incorporating advanced privacy training practices and technologies.	• Evidence of use of automation to proactively identify and report phishing attempts to relevant stakeholders	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
38. Provide any additional information on the effectiveness (positive or negative) of the organization’s data protection and privacy program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective?	N/A	N/A	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
39. To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated across the agency, and	**Ad Hoc** Roles and responsibilities have not been defined, communicated across the organization, and appropriately resourced.		Interview stakeholders to determine whether adequate resources have been planned for and provided to implement security awareness and role-based training.
	Defined Roles and responsibilities have been defined and communicated across the organization and resource requirements have been established.	• Information security program policy • Security awareness and training policies and procedures	
	Consistently Implemented Individuals are performing the roles and responsibilities that have been defined across the organization.	• IT/training budget established for agency-wide security awareness and role-based training • See additional guidance provided	
	Managed and Measurable Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to consistently implement security awareness and training responsibilities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.		
40. 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	**Ad Hoc** The organization has not defined its processes for conducting an assessment of the knowledge, skills, and abilities of its workforce.		
	Defined The organization has defined its processes for conducting an assessment of 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)	
	Consistently Implemented The organization has conducted an assessment of the knowledge, skills, and abilities of its workforce to tailor 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	
	Managed and Measurable The organization has addressed its identified knowledge, skills, and abilities gaps through the training or hiring of additional staff/contractors.	• Evidence that the agency has made progress in addressing gaps identified through its workforce assessment	
	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 being reduced over time	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
41. To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (Note: the strategy/plan should include the following components: the structure of the awareness and training program,	**<u>Ad Hoc</u>** The organization has not defined its security awareness and training strategy/plan for developing, implementing, and maintaining a security awareness and training program that is tailored to its mission and risk environment.		
	<u>Defined</u> The organization has defined its security awareness and training strategy/plan for developing, implementing, and maintaining a security awareness and training program that is tailored to its mission and risk environment.	• Security awareness and training strategy/plan	
	<u>Consistently Implemented</u> The organization has consistently implemented its organization-wide security awareness and training strategy and plan.	• Completion records for security awareness and role-based training • Cybersecurity Workforce Assessment and associated gap analysis	
	<u>Managed and Measurable</u> The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	• Evidence of tracking metrics related to security awareness and training activities	
	<u>Optimized</u> The organization's security awareness and training activities are integrated across other security-related domains. For instance, common risks and control weaknesses, and other outputs of the agency's risk management and continuous monitoring activities inform any updates that need to be made to the security awareness and training program.	• Evidence that security threats identified throughout the year are included in security awareness and training activities	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
42. To what degree have security awareness and specialized security training policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 43 and 44	**Ad Hoc** The organization has not developed, documented, and disseminated its policies and procedures for security awareness and specialized security training.		
	Defined The organization has developed, documented, and disseminated its comprehensive policies and procedures for security awareness and specialized security training that are consistent with FISMA requirements.	• Security awareness and training strategy, policies, and procedures	
	Consistently Implemented The organization consistently implements its policies and procedures for security awareness and specialized security training.	• See standard evidence for Questions #43 and #44	
	Managed and Measurable The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	• Evidence of tracking metrics related to security awareness and training activities	
	Optimized On a near real-time basis, the organization actively adapts its security awareness and training policies, procedures, and program to a changing cybersecurity landscape and provides awareness and training, as appropriate, on evolving and sophisticated threats.	• Evidence that security threats identified throughout the year are included in security awareness and training activities	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
43. To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST SP 800-53 REV. 4: AT-2; FY 2019 CIO FISMA	**Ad Hoc** The organization has not defined its security awareness material based on its organizational requirements, culture, and the types of information systems that its users have access to. In addition, the organization has not defined its processes for ensuring that all information system users are provided security awareness training prior to system access and periodically thereafter. Furthermore, the organization has not defined its processes for evaluating and obtaining feedback on its security awareness and training program and using that information to make continuous improvements.		
	Defined The organization has defined and tailored its security awareness material and delivery methods based on its organizational requirements, culture, and the types of information systems that its users have access to. In addition, the organization has defined its processes for ensuring that all information system users including contractors are provided security awareness training prior to system access and periodically thereafter. In addition, the organization has defined its processes for evaluating and obtaining feedback on its security awareness and training program and using that information to make continuous improvements.	• Security awareness content/slides/materials • Security awareness policies and procedures	
	Consistently Implemented The organization ensures that all systems users complete the organization's security awareness training (or a comparable awareness training for contractors) prior to system access and periodically thereafter and maintains completion records. The organization obtains feedback on its security awareness and training program and uses that information to make improvements.	• Evidence of tracking of security awareness completion and gathering of feedback	
	Managed and Measurable The organization measures the effectiveness of its awareness training program by, for example, conducting phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate.	• Examples of phishing exercises/emails • Evidence of tracking the results of phishing exercises and associated follow-ups	
	Optimized The organization has institutionalized a process of continuous improvement incorporating advanced security awareness practices and technologies.	• Evidence of timely updates to awareness training to account for evolving threats and risks	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
44. To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST SP 800-53 REV. 4: AT-3 and AT-4; FY 2019 CIO FISMA Metrics: 2.15)?	**Ad Hoc** The organization has not defined its security training material based on its organizational requirements, culture, and the types of roles with significant security responsibilities. In addition, the organization has not defined its processes for ensuring that all personnel with significant security roles and responsibilities are provided specialized security training prior to information system access or performing assigned duties and periodically thereafter.		
	Defined The organization has defined its security training material based on its organizational requirements, culture, and the types of roles with significant security responsibilities. In addition, the organization has defined its processes for ensuring that all personnel with assigned security roles and responsibilities are provided specialized security training prior to information system access or performing assigned duties and periodically thereafter).	• Security training content/slides/materials • Security training policies and procedures	
	Consistently Implemented The organization ensures individuals with significant security responsibilities are provided specialized security training prior to information system access or performing assigned duties and periodically thereafter and maintains appropriate records. Furthermore, the organization maintains specialized security training completion records.	• Evidence of tracking of security training completion and gathering of feedback	
	Managed and Measurable The organization obtains feedback on its security training content and makes updates to its program, as appropriate. In addition, the organization measures the effectiveness of its specialized security training program by, for example, conducting targeted phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate.	• Examples of targeted phishing exercises/emails • Evidence of tracking the results of targeted phishing exercises and associated follow-ups	
	Optimized The organization has institutionalized a process of continuous improvement incorporating advanced security training practices and technologies.	• Evidence of timely updates to security training to account for evolving threats and risks	
45. Provide any additional information on the effectiveness (positive or negative) of the organization's security training program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?	N/A	N/A	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
46. To what extent does the organization utilize an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities at each	**Ad Hoc** The organization has not developed and communicated its ISCM strategy.		At the optimized level, the outputs of the ISCM process serve as inputs to the agency's risk management, incident response, business continuity, configuration management, and other related programs on a near-real time basis.
	Defined The organization has developed and communicated its ISCM strategy that includes: i) considerations at the organization/business process level, ii) considerations at the information system level, and iii) processes to review and update the ISCM program and strategy. At the organization/business process level, the ISCM strategy defines how ISCM activities support risk management in accordance with organizational risk tolerance. At the information system level, the ISCM strategy addresses monitoring security controls for effectiveness, monitoring for security status, and reporting findings.	• ISCM strategy • ISCM policies and procedures • Agency-wide information security policy	
	Consistently Implemented The organization's ISCM strategy is 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 strategy.	• Continuous monitoring reports for selected systems • Evidence of lessons learned process	
	Managed and Measurable The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM strategy and makes updates, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	• Evidence of use of performance metrics/dashboards defined in the ISCM strategy • Evidence of verifications/validation of data feeding the metrics/dashboard	
	Optimized The organization's ISCM strategy is fully integrated with its risk management, configuration management, incident response, and business continuity functions.	• See additional guidance provided	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
47. To what extent does the organization utilize ISCM policies and procedures to facilitate organization-wide, standardized processes in support of the ISCM strategy? ISCM policies and procedures address, at a minimum, the following areas: ongoing assessments and monitoring of	**Ad Hoc** The organization has not defined its ISCM policies and procedures, at a minimum, in one or more of the specified areas.		At the optimized level, the outputs of the ISCM policies and procedures serve as inputs to the agency's risk management, incident response, business continuity, configuration management, and other related programs on a near-real time basis.
	Defined The organization's ISCM 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 requirements.	• ISCM policies and procedures • ISCM strategy	
	Consistently Implemented The organization's ISCM policies and procedures have been consistently implemented for the specified areas. The organization also consistently captures lessons learned to make improvements to the ISCM policies and procedures.	• Results of independent security control testing of select systems • POA&Ms for selected systems and at the program level • Evidence of lessons learned process	
	Managed and Measurable The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM policies and procedures and makes updates, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	• Evidence of use of performance metrics/dashboards defined in the ISCM strategy • Evidence of verifications/validation of data feeding the metrics/dashboard	
	Optimized The organization's ISCM policies and procedures are fully integrated with its risk management, configuration management, incident response, and business continuity functions.	• See additional guidance provided	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
48. To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP	**Ad Hoc** Roles and responsibilities have not been fully defined and communicated across the organization, including appropriate levels of authority and dependencies.		
	Defined The organization has defined and communicated the structures of its ISCM team, roles and responsibilities of ISCM stakeholders, and levels of authority and dependencies.	• Information security program policy • ISCM strategy, policies, and procedures • Organizational charts • Delegations of authority	
	Consistently Implemented Individuals are performing the roles and responsibilities that have been defined across the organization.	• Evidence that individuals are assigned ISCM responsibilities are carrying out their duties at the system level • Agency's IT security budget	
	Managed and Measurable Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement ISCM activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	• Evidence of use of performance metrics/dashboards defined in the ISCM strategy • Evidence of verifications/validation of data feeding the metrics/dashboard	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
49. How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls (NIST SP 800-137: Section 2.2; NIST SP 800-53 REV. 4: CA-2, CA-6, and CA-7; NIST	**Ad Hoc** The organization has not defined its processes for performing ongoing security control assessments, granting system authorizations, and monitoring security controls for individual systems.		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.
	Defined The organization has defined its processes for performing ongoing security control assessments, granting system authorizations, and monitoring security controls for individual systems.	• ISCM strategy • ISCM policies and procedures • Agency-wide information security policy	
	Consistently Implemented The organization has consistently implemented its processes for performing ongoing security control assessments, granting system authorizations, and monitoring security controls to provide a view of the organizational security posture as well as each system's contribution to said security posture. All security control classes (management, operational, technical) and types (common, hybrid, and system-specific) are assessed and monitored.	• Evidence of ongoing security control assessments for a sample of systems at the appropriate level of rigor and frequency • Evidence of system authorizations for select systems (including POA&Ms, SSPs, SARs, and ATO letters) • Organization-wide risk management strategy, appetite, and tolerance	
	Managed and Measurable The organization utilizes the results of security control assessments and monitoring to maintain ongoing authorizations of information systems.	• Evidence of the generation and collection of security-related information for all implemented security controls, including inherited common controls, at the frequencies specified in the ISCM strategy	
	Optimized The ISCM program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact.	• See additional guidance provided	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
50. How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?	**Ad Hoc** The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. Further, the organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk based decisions.		
	Defined The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. In addition, the organization has defined the format of reports, frequency of reports, and the tools used to provide information to individuals with significant security responsibilities.	• ISCM strategy • ISCM policies and procedures • Agency-wide information security policy	
	Consistently Implemented The organization is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting.	• Evidence of use of performance metrics/dashboards defined in the ISCM strategy • Evidence of verifications/validation of data feeding the metrics/dashboard	
	Managed and Measurable The organization is able to integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations and security domains.	• Evidence of an integrated dashboarding capability that captures inputs from ISCM and other related security domains and offers the capability to see security status across the organization	
	Optimized On a near real-time basis, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.	• Evidence of near-real time updates using the updates of the agency's integrated dashboarding capability	
51. Provide any additional information on the effectiveness (positive or negative) of the organization's ISCM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?	N/A	N/A	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
52. To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events (NIST SP 800-53 REV. 4: IR-1; NIST SP 800-61 Rev. 2; NIST SP 800-184; OMB M-17-25; OMB M-17-09; FY 2018 CIO FISMA Metrics: 4.2; CSF: RS.RP-1; Presidential Policy Direction (PPD) 41)? (Note: The overall maturity level should take into consideration the maturity of questions 53 - 58).	**Ad Hoc** The organization has not defined its incident response policies, procedures, plans, and strategies in one or more of the following areas: incident response planning, to include organizational specific considerations for major incidents, incident response training and testing, incident detection and analysis, incident containment, eradication, and recovery; incident coordination, information sharing, and reporting.		At the optimized level, the outputs of the incident response process serve as inputs to the agency's risk management, ISCM, business continuity, configuration management, and other related programs on a near-real time basis.
	Defined The organization's incident response policies, procedures, plans, and strategies have been defined and communicated. In addition, the organization has established and communicated an enterprise level incident response plan.	• Incident response strategies, policies, procedures, and standards • Enterprise-level incident response plan • Evidence of communication of the incident response plan through training or other means	
	Consistently Implemented The organization consistently implements its incident response policies, procedures, plans, and strategies. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident response policies, procedures, strategy and processes to update the program.	• See standard source evidence for Questions #54 - #58	
	Managed and Measurable The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.	• Evidence of use of performance metrics/dashboards defined in the incident response plan, policies, procedures, and strategy • Evidence of verifications/validation of data feeding the metrics/dashboard	
	Optimized The organization's incident response program, policies, procedures, strategies, plans are related activities are fully integrated with risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate.	• See additional guidance provided	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
53. To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: IR-7; NIST SP 800-	**Ad Hoc** Roles and responsibilities have not been fully defined and communicated across the organization, including appropriate levels of authority and dependencies.		
	Defined The organization has defined and communicated the structures of its incident response teams, roles and responsibilities of incident response stakeholders, and associated levels of authority and dependencies. In addition, the organization has designated a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities.	• Incident response strategies, policies, procedures, and standards • Enterprise-level incident response plan • Organizational chart showing a breakdown of the incident response function • Charters for any organization-wide committees involved in incident response functions	
	Consistently Implemented Individuals are performing the roles and responsibilities that have been defined across the organization.	• Based on select incident tickets, evidence that processes were followed (e.g., reporting to US-CERT, reporting to internal stakeholders, etc.) • IT security budget, including considerations for the technologies defined in Question #58	
	Managed and Measurable Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement incident response activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.	• Evidence of use of performance metrics defined in the incident response policies, procedures, and plan • Evidence of verifications/validation of data feeding the metrics	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
54. How mature are the organization's processes for incident detection and analysis? (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-18-02; CSF: DE.AE-1, PR.DS-6, RS.AN-4, and PR.DS-8; and US-CERT Incident Response Guidelines)	**Ad Hoc** The organization has not defined a common threat vector taxonomy for classifying incidents and its processes for detecting, analyzing, and prioritizing incidents.		At the consistently implemented level, perform observation of technologies and tools supporting incident detection and analysis to verify whether the defined indicators and precursors are being captured and reviewed.
	Defined 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 response strategies, policies, procedures, and standards • 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 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 detection/prevention, security information and event management (SIEM), antivirus and antispam software, and file integrity checking software.	• Sample of incident tickets, including those submitted to US-CERT • For the tools listed in Question #58, evidence of configurations that show the precursors and indicators captured	
	Managed and Measurable 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.	• Baseline of expected data flows and network operations • Evidence of use of checksums for critical files	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
55. How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2)	**Ad Hoc** The organization has not defined its processes for incident handling to include: containment strategies for various types of major incidents, eradication activities to eliminate components of an incident and mitigate any vulnerabilities that were exploited, and recovery of systems.		At the optimized level, observe technologies in use for dynamic reconfiguration of network devices in response to incident types.
	Defined The organization has developed containment strategies for each major 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 • Incident response policies, procedures, and plans	
	Consistently Implemented The organization consistently implements its containment strategies, incident eradication processes, processes to remediate vulnerabilities that may have been exploited on the target system(s), and recovers system operations.	• Sample of incident tickets to obtain evidence that containment strategies were followed • Evidence that vulnerabilities that were exploited and resulted in incidents were remediated (e.g., vulnerability scanning reports, or additional training)	
	Managed and Measurable The organization manages and measures the impact of successful incidents and is able to 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	
	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.	• See additional guidance provided	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
56. To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-18-02; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 4; DHS Cyber Incident Reporting Unified Message)	**Ad Hoc** The organization has not defined how incident response information will be shared with individuals with significant security responsibilities or its processes for reporting security incidents to US-CERT and other stakeholders (e.g., Congress and the Inspector General, as applicable) in a timely manner.		
	Defined The organization has defined its requirements for personnel to report suspected security incidents to the organization's incident response capability within organization defined timeframes. In addition, the organization has defined its processes for reporting security incident information to US-CERT, law enforcement, the Congress (for major incidents) and the Office of Inspector General, as appropriate.	• Incident response strategies, policies, procedures, and standards • Enterprise-level incident response plan • Content of security awareness and role-based training	
	Consistently Implemented The organization consistently shares information on incident activities with internal stakeholders. The organization ensures that security incidents are reported to US-CERT, law enforcement, the Office of Inspector General, and the Congress (for major incidents) in a timely manner.	• Meeting minutes of any committees involved in incident response • Sample of incident response tickets, including timestamps for communication and notification • Corresponding US-CERT incident response tickets, per your sample • List of major incidents and corresponding reporting to Congress, as applicable • Evidence of participation in Eagle Horizon exercises	
	Managed and Measurable Incident response metrics are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.	• 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	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
57. To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support (NIST SP 800-86; NIST SP 800-53 REV. 4: IR-4; OMB M-18-02; PPD-41).	**Ad Hoc** The organization has not defined how it will collaborate with DHS and other parties, as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. In addition, the organization has not defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks.		At the consistently implemented level, evaluate the agency's timeliness of requested incident response services and assess the agency's quality of the services being provided.
	Defined The organization has defined how it will collaborate with DHS and other parties, as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. This includes identification of incident response services that may need to be procured to support organizational processes. In addition, the organization has defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks.	• Contracts/Task Orders/SOWs/service level agreements for incident response services • MOAs/MOUs with DHS • Incident response plan	
	Consistently Implemented The organization consistently utilizes on-site, technical assistance/surge capabilities offered by DHS or ensures that such capabilities are in place and can be leveraged when needed. In addition, the organization has entered into contractual relationships in support of incident response processes (e.g., for forensic support), as needed. The organization has fully deployed DHS' Einstein 1 and 2 to screen all traffic entering and leaving its network through a TIC.	• Evidence of monitoring feeds from DHS related to Einstein 1 and 2 • See additional guidance provided	
	Managed and Measurable The organization utilizes Einstein 3 Accelerated to detect and proactively block cyber-attacks or prevent potential compromises.	• Evidence of monitoring feeds from DHS related to Einstein 3A	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
58. To what degree does the organization utilize the following technology to support its incident response program? -Web application protections, such as web application firewalls -Event and incident management, such as intrusion	**Ad Hoc** The organization has not identified and defined its requirements for incident response technologies needed in one or more of the specified areas and relies on manual/procedural methods in instances where automation would be more effective.		At the consistently implemented level, observe the technologies being used to verify coverage of the organization's network and the extent to which they are interoperable. Further, observe whether the tools are able to identify the source and the target(s) of the information being flagged.
	Defined The organization has identified and fully defined its requirements for the incident response technologies it plans to utilize in the specified areas. While tools are implemented to support some incident response activities, the tools are not interoperable to the extent practicable, do not cover all components of the organization’s network, and/or have not been configured to collect and retain relevant and meaningful data consistent with the organization’s incident response policy, plans, and procedures.	• Incident response plan and strategies, including defined requirements for the incident response program • SOPs for the tools being used • Network architecture diagram	
	Consistently Implemented The organization has consistently implemented its defined incident response technologies in the specified areas. In addition, the technologies utilized are interoperable to the extent practicable, cover all components of the organization's network, and have been configured to collect and retain relevant and meaningful data consistent with the organization’s incident response policy, procedures, and plans.	• List of feeds into the agency's SIEM tool • See additional guidance provided	
	Managed and Measurable The organization uses technologies for monitoring and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing incident response activities.	• Evidence of use of performance metrics/dashboards defined in the incident response policies, procedures, and plan • Evidence of verifications/validation of data feeding the metrics/dashboards	
	Optimized The organization has institutionalized the implementation of advanced incident response technologies for analysis of trends and performance against benchmarks (e.g., simulation based technologies to continuously determine the impact of potential security incidents to its IT assets) and adjusts incident response processes and security measures accordingly.	• Results of trend analysis, benchmarking, and the resulting updates made to the incident response program • Evidence of use of simulation technologies to model the impact of an incident on the agency's environment	
59. Provide any additional information on the effectiveness (positive or negative) of the organization’s incident response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?	N/A	N/A	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
60. To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined and communicated across the organization, including appropriate delegations of authority (NIST SP 800-53 REV. 4: CP-1 and CP-2; NIST SP 800-34; NIST SP 800-84; FCD-1; Annex B)?	**Ad Hoc** Roles and responsibilities have not been fully defined and communicated across the organization, including appropriate delegations of authority.		At the consistently implemented level, the CIO/CISO have enterprise-wide visibility into contingency planning activities and any associated gaps that may need resources directed to them. Further, plans have been established to close those identified gaps.
	Defined Roles and responsibilities of stakeholders have been fully defined and communicated across the organization, including appropriate delegations of authority. In addition, the organization has designated appropriate teams to implement its contingency planning strategies. Further, the organization has assigned responsibility for monitoring and tracking the effectiveness of information systems contingency planning activities.	• Information security policy • Information system contingency planning policies and procedures • Agency-wide COOP, BCP, and DR plans, policies, and procedures • Delegations of authority • Organizational chart	
	Consistently Implemented The organization has established appropriate teams that are ready to implement its information system contingency planning strategies. Stakeholders and teams have adequate resources (people, processes, and technology) to effectively implement system contingency planning activities. Individuals are performing the roles and responsibilities that have been defined across the organization.	• POA&Ms • Sample after-action reports for contingency exercises • See additional guidance provided	
	Managed and Measurable Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement system contingency planning activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.		

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
61. To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate (Note: Assignment of an overall maturity level should take into consideration the maturity of questions 62-66) (NIST SP 800-34; NIST SP 800-161; CSF: ID.BE-5, PR.IP-9, and ID.SC-5).	**Ad Hoc** The organization has not defined its policies, procedures, and strategies, as appropriate, for information system contingency planning. Policies/procedures/strategies do not sufficiently address, at a minimum, the following areas: roles and responsibilities, scope, resource requirements, training, exercise and testing schedules, plan maintenance, technical contingency planning considerations for specific types of systems, schedules, backups and storage, and use of alternate processing and storage sites.		For the managed and measurable level, the organization has integrated ICT supply chain concerns and risks into its contingency planning program, including planning for alternative suppliers of system components, alternative suppliers of systems and services, denial of service attacks to the supply chain, and planning for alternative delivery routes for critical system components. At the optimized level, the outputs of the contingency planning policies and procedures serve as inputs to the agency's enterprise risk management program, strategic
	Defined The organization has defined its policies, procedures, and strategies, as appropriate, for information system contingency planning, including technical contingency planning considerations for specific types of systems, such as cloud-based systems, client/server, telecommunications, and mainframe based systems. Areas covered include, at a minimum, roles and responsibilities, scope, resource requirements, training, exercise and testing schedules, plan maintenance schedules, backups and storage, and use of alternate processing and storage sites.	• Information security policy • Information system contingency planning policies and procedures • Agency-wide COOP, BCP, and DR plans, policies, and procedures	
	Consistently Implemented The organization consistently implements its defined information system contingency planning policies, procedures, and strategies. In addition, the organization consistently implements technical contingency planning considerations for specific types of systems, including but not limited to methods such as server clustering and disk mirroring. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of information system contingency planning policies, procedures, strategy, and processes to update the program.	• See standard source evidence for Questions #52 - #56	
	Managed and Measurable The organization understands and manages its information and communications technology (ICT) supply chain risks related to contingency planning activities. As appropriate, the organization: integrates ICT supply chain concerns into its contingency planning policies and procedures, defines and implements a contingency plan for its ICT supply chain infrastructure, applies appropriate ICT supply chain controls to alternate storage and processing sites, considers alternate telecommunication service providers for its ICT supply chain infrastructure and to support critical information systems.	• ICT supply chain infrastructure contingency plan • See additional guidance provided	
	Optimized The information system contingency planning program is fully integrated with the enterprise risk management program, strategic planning processes, capital allocation/budgeting, and other mission/business areas and embedded into daily decision making across the organization.	• See additional guidance provided	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
62. To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17-09; FY 2019 CIO FISMA Metrics: 5.1; CSF:ID.RA-4)?	**Ad hoc** Processes for conducting organizational and system-level BIAs and for incorporating the results into strategy and plan development efforts have not been defined in policies and procedures and are performed in an ad-hoc, reactive manner.		
	Defined Processes for conducting organizational and system-level BIAs and for incorporating the results into strategy and plan development efforts have been defined.	• Information security policy • Information system contingency planning policies and procedures • Templates for completing BIAs	
	Consistently Implemented The organization incorporates the results of organizational and system level BIAs into strategy and plan development efforts consistently. System level BIAs are integrated with the organizational level BIA and include: characterization of all system components, determination of missions/business processes and recovery criticality, identification of resource requirements, and identification of recovery priorities for system resources. The results of the BIA are consistently used to determine contingency planning requirements and priorities, including mission essential functions/high-value assets.	• Organizational level BIA • Sample of system level BIAs	
63. To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34; FY 2019 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?	**Ad Hoc** Processes for information system contingency plan development and maintenance have not been defined in policies and procedures; the organization has not developed templates to guide plan development; and system contingency plans are developed in an ad-hoc manner with limited integration with other continuity plans.		At the optimized level, the outputs of the contingency planning policies and procedures serve as inputs to the agency's enterprise risk management program, strategic planning processes, capital allocation/budgeting, and other mission/business areas on a near-real time basis.
	Defined Processes for information system contingency plan development, maintenance, and integration with other continuity areas have been defined and include the following phases: activation and notification, recovery, and reconstitution.	• Information security policy • Information system contingency planning policies and procedures	
	Consistently Implemented Information system contingency plans are consistently developed and implemented for systems, as appropriate, and include organizational and system level considerations for the following phases: activation and notification, recovery, and reconstitution. In addition, system level contingency planning development/maintenance activities are integrated with other continuity areas including organization and business process continuity, disaster recovery planning, incident management, insider threat implementation plan (as appropriate), and occupant emergency plans.	• For select systems, system-specific contingency plans • Disaster Recovery Plan, Incident Response Plan, COOP, and Insider Threat Implementation Plan, Occupant Emergency Plan	
	Managed and Measurable The organization is able to integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency, as appropriate to deliver persistent situational awareness across the organization.	• Evidence of use of performance metrics/dashboards • Evidence of verifications/validation of data feeding the metrics/dashboard	
	Optimized The information system contingency planning activities are fully integrated with the enterprise risk management program, strategic planning processes, capital allocation/budgeting, and other mission/business areas and embedded into daily decision making across the organization.	• See additional guidance provided	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
64. To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53 REV. 4: CP-3 and CP-4; FY 2019 CIO FISMA Metrics: 5.1; CSF: ID.SC-5 and CSF: PR.IP-	**Ad Hoc** Processes for information system contingency plan testing/exercises have not been defined and contingency plan tests for systems are performed in an ad-hoc, reactive manner.		At the managed and measurable level, automated mechanisms provide more thorough and effective testing of contingency plans, for example: (i) by providing more complete coverage of contingency
	Defined Processes for information system contingency plan testing and exercises have been defined and include, as applicable, notification procedures, system recovery on an alternate platform from backup media, internal and external connectivity, system performance using alternate equipment, restoration of normal procedures, and coordination with other business areas/continuity plans, and tabletop and functional exercises.	• Information security policy • Information system contingency planning policies and procedures	
	Consistently Implemented Processes for 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 more thoroughly and effectively test system contingency plans. In addition, the organization coordinates plan testing with external stakeholders (e.g., ICT supply chain partners/providers), as appropriate.	• See additional guidance provided	
	Optimized The organization coordinates information system contingency plan testing with organizational elements responsible for related plans.	• ISCP testing results for selected systems • Results of testing of COOP, BCP, DRP, and OEP • See additional guidance provided	
65. To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 800-53 REV. 4: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD-1; NIST CSF: PR.IP-4; FY 2019 CIO FISMA Metrics: 5.1.1; and NARA guidance on information systems security records)?	**Ad Hoc** Processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and redundant array of independent disks (RAID), as appropriate, have not been defined. Information system backup and storage is performed in an ad- hoc, reactive manner.		
	Defined Processes, strategies, and technologies for information system backup and storage, including use of alternate storage and processing sites and RAID, as appropriate, have been defined. The organization has considered alternative approaches when developing its backup and storage strategies, including cost, maximum downtimes, recovery priorities, and integration with other contingency plans.	• Information security policy • Information system contingency planning policies and procedures	
	Consistently Implemented The organization consistently implements its processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and RAID, as appropriate. Alternate processing and storage sites are chosen based upon risk assessments which ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized, and are not subject to the same physical and/or cybersecurity risks as the primary sites. In addition, the organization ensures that alternate processing and storage facilities are configured with information security safeguards equivalent to those of the primary site. Furthermore, backups of information at the user- and system-levels are consistently performed and the confidentiality, integrity, and availability of this information is maintained.	• For select systems, obtain SSPs and ISCPs • Evidence of risk assessment being performed to guide the selection of alternative storage and processing sites of applicable systems • Results of independent testing and continuous monitoring reports of the alternate processing and storage facilities • For select systems, evidence of user- and system-level backups for a defined timeframe	

IG Metric - FY18	Maturity Level	Suggested Standard Source Evidence	Additional Guidance
66. To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk based decisions (CSF: RC.CO-3; NIST SP 800-53 REV. 4: CP-2 and IR-4)?	**Ad Hoc** The organization has not defined how the planning and performance of recovery activities are communicated to internal stakeholders and executive management teams and used to make risk based decisions.		
	Defined The organization has defined how the planning and performance of recovery activities are communicated to internal stakeholders and executive management teams.	• Information security policy • Information system contingency planning policies and procedures • ISCP (and related plans) testing schedule	
	Consistently Implemented Information on the planning and performance of recovery activities is consistently communicated to relevant stakeholders and executive management teams, who utilize the information to make risk based decisions.	• Evidence of communication of recovery activities (e.g., after-action reports, POA&Ms, etc.) to contingency planning stakeholders for coordinated testing/activities • Evidence showing that items within after-action reports are remediated	
	Managed and Measurable Metrics on the effectiveness of recovery activities are communicated to relevant stakeholders and the organization has ensured that the data supporting the metrics are obtained accurately, consistently, and in a reproducible format.	• Evidence of use of performance metrics/dashboards • Evidence of verifications/validation of data feeding the metrics/dashboard	
67. Provide any additional information on the effectiveness (positive or negative) of the organization's contingency planning program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the contingency program effective?	N/A	N/A	