NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **NIST SP 800-161 R1 UDP1 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations**
Focal Document URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-161-r1-level-1.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description NIST SP 800-161 R1 Supplemental C-SCRM Guidance	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
AC-1	Policy and Procedures	Enterprises should specify and include in agreements (e.g., contracting language) access control policies for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers that have access control policies. These should include both physical and logical access to the supply chain and the information system. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtier contractors.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AC-1	Policy and Procedures	Enterprises should specify and include in agreements (e.g., contracting language) access control policies for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers that have access control policies. These should include both physical and logical access to the supply chain and the information system. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtier contractors.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AC-1	Policy and Procedures	Enterprises should specify and include in agreements (e.g., contracting language) access control policies for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers that have access control policies. These should include both physical and logical access to the supply chain and the information system. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtier contractors.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AC-18	Wireless Access	An enterprise’s supply chain may include wireless infrastructure that supports supply chain logistics (e.g., radio-frequency identification device [RFID] support, software call home features). Supply chain systems/components traverse the supply chain as they are moved from one location to another, whether within the enterprise’s own environment or during delivery from system integrators or suppliers. Ensuring that appropriate and secure access mechanisms are in place within this supply chain enables the protection of the information systems and components, as well as logistics technologies and metadata used during shipping (e.g., within tracking sensors). The enterprise should explicitly define appropriate wireless access control mechanisms for the supply chain in policy and implement appropriate mechanisms.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and b. Authorize each type of wireless access to the system prior to allowing such connections.
AC-18	Wireless Access	An enterprise’s supply chain may include wireless infrastructure that supports supply chain logistics (e.g., radio-frequency identification device [RFID] support, software call home features). Supply chain systems/components traverse the supply chain as they are moved from one location to another, whether within the enterprise’s own environment or during delivery from system integrators or suppliers. Ensuring that appropriate and secure access mechanisms are in place within this supply chain enables the protection of the information systems and components, as well as logistics technologies and metadata used during shipping (e.g., within tracking sensors). The enterprise should explicitly define appropriate wireless access control mechanisms for the supply chain in policy and implement appropriate mechanisms.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and b. Authorize each type of wireless access to the system prior to allowing such connections.
AC-20	Use of External Systems	Enterprises’ external information systems include those of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Unlike in an acquirer’s internal enterprise where direct and continuous monitoring is possible, in the external supplier relationship, information may be shared on an as-needed basis and should be articulated in an agreement. Access to the supply chain from such external information systems should be monitored and audited. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Equal	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	10	a. [Selection (one or more): Establish [Assignment: organization-defined terms and conditions]; Identify [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:
AC-21	Information Sharing	Sharing information within the supply chain can help manage cybersecurity risks throughout the supply chain. This information may include vulnerabilities, threats, the criticality of systems and components, or delivery information. This information sharing should be carefully managed to ensure that the information is only accessible to authorized individuals within the enterprise’s supply chain. Enterprises should clearly define boundaries for information sharing with respect to temporal, informational, contractual, security, access, system, and other requirements. Enterprises should monitor and review for unintentional or intentional information sharing within its supply chain activities, including information sharing with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Intersects With	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	5	a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information’s access and use restrictions for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and b. Employ [Assignment: organization-defined automated mechanisms or manual processes] to
AC-21	Information Sharing	Sharing information within the supply chain can help manage cybersecurity risks throughout the supply chain. This information may include vulnerabilities, threats, the criticality of systems and components, or delivery information. This information sharing should be carefully managed to ensure that the information is only accessible to authorized individuals within the enterprise’s supply chain. Enterprises should clearly define boundaries for information sharing with respect to temporal, informational, contractual, security, access, system, and other requirements. Enterprises should monitor and review for unintentional or intentional information sharing within its supply chain activities, including information sharing with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Intersects With	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5	a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information’s access and use restrictions for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and b. Employ [Assignment: organization-defined automated mechanisms or manual processes] to
AC-24	Access Control Decisions	Enterprises should assign access control decisions to support authorized access to the supply chain. Ensure that if a system integrator or external service provider is used, there is consistency in access control decision requirements and how the requirements are implemented. This may require defining such requirements in service-level agreements, in many cases as part of the upfront relationship established between the enterprise and system integrator or the enterprise and external service provider. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	5	[Selection: Establish procedures; Implement mechanisms] to ensure [Assignment: organization-defined access control decisions] are applied to each access request prior to access enforcement.
AT-1	Policy and Procedures	responsibilities. Enterprises should integrate cybersecurity supply chain risk management training and awareness into the security training and awareness policy. C-SCRM training should target both the enterprise and its contractors. The policy should ensure that supply chain cybersecurity role-based training is required for those individuals or functions that touch or impact the supply chain, such as the information system owner, acquisition, supply chain logistics, system engineering, program management, IT, quality, and incident response. C-SCRM training procedures should address: a. Roles throughout the supply chain and system/element life cycle to limit the opportunities and means available to individuals performing these roles that could result in adverse consequences,	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AT-1	Policy and Procedures	responsibilities. Enterprises should integrate cybersecurity supply chain risk management training and awareness into the security training and awareness policy. C-SCRM training should target both the enterprise and its contractors. The policy should ensure that supply chain cybersecurity role-based training is required for those individuals or functions that touch or impact the supply chain, such as the information system owner, acquisition, supply chain logistics, system engineering, program management, IT, quality, and incident response. C-SCRM training procedures should address: a. Roles throughout the supply chain and system/element life cycle to limit the opportunities and means available to individuals performing these roles that could result in adverse consequences,	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AT-1	Policy and Procedures	responsibilities. Enterprises should integrate cybersecurity supply chain risk management training and awareness into the security training and awareness policy. C-SCRM training should target both the enterprise and its contractors. The policy should ensure that supply chain cybersecurity role-based training is required for those individuals or functions that touch or impact the supply chain, such as the information system owner, acquisition, supply chain logistics, system engineering, program management, IT, quality, and incident response. C-SCRM training procedures should address: a. Roles throughout the supply chain and system/element life cycle to limit the opportunities and means available to individuals performing these roles that could result in adverse consequences,	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AU-1	Policy and Procedures	Enterprises must designate a specific official to manage the development, documentation, and dissemination of the audit and accountability policy and procedures to include auditing of the supply chain information systems and network. The audit and accountability policy and procedures should appropriately address tracking activities and their availability for other various supply chain activities, such as configuration management. Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers activities should not be included in such a policy unless those functions are performed within the acquirer’s supply chain information systems and network. Audit and accountability policy procedures should appropriately address supplier audits as a way to examine the quality of a particular supplier and the risk they present to the enterprise and the enterprise’s	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AU-1	Policy and Procedures	Enterprises must designate a specific official to manage the development, documentation, and dissemination of the audit and accountability policy and procedures to include auditing of the supply chain information systems and network. The audit and accountability policy and procedures should appropriately address tracking activities and their availability for other various supply chain activities, such as configuration management. Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers activities should not be included in such a policy unless those functions are performed within the acquirer’s supply chain information systems and network. Audit and accountability policy procedures should appropriately address supplier audits as a way to examine the quality of a particular supplier and the risk they present to the enterprise and the enterprise’s	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AU-1	Policy and Procedures	Enterprises must designate a specific official to manage the development, documentation, and dissemination of the audit and accountability policy and procedures to include auditing of the supply chain information systems and network. The audit and accountability policy and procedures should appropriately address tracking activities and their availability for other various supply chain activities, such as configuration management. Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers activities should not be included in such a policy unless those functions are performed within the acquirer’s supply chain information systems and network. Audit and accountability policy procedures should appropriately address supplier audits as a way to examine the quality of a particular supplier and the risk they present to the enterprise and the enterprise’s	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AU-2	Event Logging	software/hardware changes, failed attempts to access supply chain information systems, or the movement of source code. Information on such events should be captured by appropriate audit mechanisms and be traceable and verifiable. Information captured may include the type of event, date/time, length, and the frequency of occurrence. Among other things, auditing may help detect misuse of the supply chain information systems or network caused by insider threats. Logs are a key resource when identifying operational trends and long-term problems. As such, enterprises should incorporate reviewing logs at the contract renewal point for vendors to determine whether there is a systemic problem. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
AU-2	Event Logging	software/hardware changes, failed attempts to access supply chain information systems, or the movement of source code. Information on such events should be captured by appropriate audit mechanisms and be traceable and verifiable. Information captured may include the type of event, date/time, length, and the frequency of occurrence. Among other things, auditing may help detect misuse of the supply chain information systems or network caused by insider threats. Logs are a key resource when identifying operational trends and long-term problems. As such, enterprises should incorporate reviewing logs at the contract renewal point for vendors to determine whether there is a systemic problem. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
AU-3	Content of Audit Records	The audit records of a supply chain event should be securely handled and maintained in a manner that conforms to record retention requirements and preserves the integrity of the findings and the confidentiality of the record information and its sources as appropriate. In certain instances, such records may be used in administrative or legal proceedings. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation’s Cybersecurity.	Functional	Equal	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and	10	Ensure that audit records contain information that establishes the following: a. What type of event occurred; b. When the event occurred; c. Where the event occurred; d. Source of the event; e. Outcome of the event; and f. Identity of any individuals, subjects, or
CA-1	Policy and Procedures	Integrate the development and implementation of assessment and authorization policies and procedures for supply chain cybersecurity into the control assessment and authorization policy and related C-SCRM Strategy/Implementation Plan(s), policies, and system-level plans. To address cybersecurity risks throughout the supply chain, enterprises should develop a C-SCRM policy (or, if required, integrate into existing policies) to direct C-SCRM activities for control assessment and authorization. The C-SCRM policy should define C-SCRM roles and responsibilities within the enterprise for conducting control assessment and authorization, any dependencies among those roles, and the interaction among the roles. Enterprise-wide security and privacy risks should be assessed on an ongoing basis and include supply chain risk assessment results.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that: (a) Addresses purpose, scope, roles, responsibilities,
CA-1	Policy and Procedures	Integrate the development and implementation of assessment and authorization policies and procedures for supply chain cybersecurity into the control assessment and authorization policy and related C-SCRM Strategy/Implementation Plan(s), policies, and system-level plans. To address cybersecurity risks throughout the supply chain, enterprises should develop a C-SCRM policy (or, if required, integrate into existing policies) to direct C-SCRM activities for control assessment and authorization. The C-SCRM policy should define C-SCRM roles and responsibilities within the enterprise for conducting control assessment and authorization, any dependencies among those roles, and the interaction among the roles. Enterprise-wide security and privacy risks should be assessed on an ongoing basis and include supply chain risk assessment results.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that: (a) Addresses purpose, scope, roles, responsibilities,
CA-1	Policy and Procedures	Integrate the development and implementation of assessment and authorization policies and procedures for supply chain cybersecurity into the control assessment and authorization policy and related C-SCRM Strategy/Implementation Plan(s), policies, and system-level plans. To address cybersecurity risks throughout the supply chain, enterprises should develop a C-SCRM policy (or, if required, integrate into existing policies) to direct C-SCRM activities for control assessment and authorization. The C-SCRM policy should define C-SCRM roles and responsibilities within the enterprise for conducting control assessment and authorization, any dependencies among those roles, and the interaction among the roles. Enterprise-wide security and privacy risks should be assessed on an ongoing basis and include supply chain risk assessment results.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that: (a) Addresses purpose, scope, roles, responsibilities,
CA-6	Authorization	Authorizing officials should include C-SCRM in authorization decisions. To accomplish this, supply chain risks and compensating controls documented in C-SCRM Plans or system security plans and the C-SCRM POA&M should be included in the authorization package as part of the decision-making process. Risks should be determined and associated compensating controls selected based on the output of criticality, threat, and vulnerability analyses. Authorizing officials may use the guidance in Section 2 of this document as well as NISTIR 8179 to guide the assessment process.	Functional	Equal	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	10	a. Assign a senior official as the authorizing official for the system; b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems; c. Ensure that the authorizing official for the system, before commencing operations: 1. Accepts the use of common controls inherited by
CM-1	Policy and Procedures	to the enterprise’s ability to establish the provenance of components, including tracking and tracing them through the SDLC and the supply chain. A properly defined and implemented configuration management capability provides greater assurance throughout the SDLC and the supply chain that components are authentic and have not been inappropriately modified. When defining a configuration management policy and procedures, enterprises should address the full SDLC, including procedures for introducing and removing components to and from the enterprise’s information system boundary. A configuration management policy should incorporate configuration items, data retention for configuration items and corresponding metadata, and tracking of the configuration item and its metadata. The enterprise should coordinate with suppliers, developers, system integrators, external system	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
CM-1	Policy and Procedures	to the enterprise’s ability to establish the provenance of components, including tracking and tracing them through the SDLC and the supply chain. A properly defined and implemented configuration management capability provides greater assurance throughout the SDLC and the supply chain that components are authentic and have not been inappropriately modified. When defining a configuration management policy and procedures, enterprises should address the full SDLC, including procedures for introducing and removing components to and from the enterprise’s information system boundary. A configuration management policy should incorporate configuration items, data retention for configuration items and corresponding metadata, and tracking of the configuration item and its metadata. The enterprise should coordinate with suppliers, developers, system integrators, external system	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
CM-1	Policy and Procedures	to the enterprise’s ability to establish the provenance of components, including tracking and tracing them through the SDLC and the supply chain. A properly defined and implemented configuration management capability provides greater assurance throughout the SDLC and the supply chain that components are authentic and have not been inappropriately modified. When defining a configuration management policy and procedures, enterprises should address the full SDLC, including procedures for introducing and removing components to and from the enterprise’s information system boundary. A configuration management policy should incorporate configuration items, data retention for configuration items and corresponding metadata, and tracking of the configuration item and its metadata. The enterprise should coordinate with suppliers, developers, system integrators, external system	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
CP-1	Policy and Procedures	Enterprises should integrate C-SCRM into the contingency planning policy and related SCRM Strategy/Implementation Plan, policies, and SCRM Plan. The policy should cover information systems and the supply chain network and, at a minimum, address scenarios such as: a. Unplanned component failure and subsequent replacement; b. Planned replacement related to feature improvements, maintenance, upgrades, and modernization; and c. Product and/or service disruption.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
CP-1	Policy and Procedures	Enterprises should integrate C-SCRM into the contingency planning policy and related SCRM Strategy/Implementation Plan, policies, and SCRM Plan. The policy should cover information systems and the supply chain network and, at a minimum, address scenarios such as: a. Unplanned component failure and subsequent replacement; b. Planned replacement related to feature improvements, maintenance, upgrades, and modernization; and c. Product and/or service disruption.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among

FDE #	FDE Name	Focal Document Element (FDE) Description NIST SP 800-161 R1 Supplemental C-SCRM Guidance	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
CP-1	Policy and Procedures	Enterprises should integrate C-SCRM into the contingency planning policy and related SCRM Strategy/Implementation Plan, policies, and SCRM Plan. The policy should cover information systems and the supply chain network and, at a minimum, address scenarios such as: a. Unplanned component failure and subsequent replacement; b. Planned replacement related to feature improvements, maintenance, upgrades, and modernization; and c. Product and/or service disruption.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IA-1	Policy and Procedures	The enterprise should – at enterprise-defined intervals – review, enhance, and update their identity and access management policies and procedures to ensure that critical roles and processes within the supply chain network are defined and that the enterprise's critical systems, components, and processes are identified for traceability. This should include the identity of critical components that may not have been considered under identification and authentication in the past. Note that providing identification for all items within the supply chain would be cost-prohibitive, and discretion should be used. The enterprise should update related C-SCRM Strategy/Implementation Plan(s), Policies, and C-SCRM Plans.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IA-1	Policy and Procedures	The enterprise should – at enterprise-defined intervals – review, enhance, and update their identity and access management policies and procedures to ensure that critical roles and processes within the supply chain network are defined and that the enterprise's critical systems, components, and processes are identified for traceability. This should include the identity of critical components that may not have been considered under identification and authentication in the past. Note that providing identification for all items within the supply chain would be cost-prohibitive, and discretion should be used. The enterprise should update related C-SCRM Strategy/Implementation Plan(s), Policies, and C-SCRM Plans.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IA-1	Policy and Procedures	The enterprise should – at enterprise-defined intervals – review, enhance, and update their identity and access management policies and procedures to ensure that critical roles and processes within the supply chain network are defined and that the enterprise's critical systems, components, and processes are identified for traceability. This should include the identity of critical components that may not have been considered under identification and authentication in the past. Note that providing identification for all items within the supply chain would be cost-prohibitive, and discretion should be used. The enterprise should update related C-SCRM Strategy/Implementation Plan(s), Policies, and C-SCRM Plans.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IA-2	Identification and Authentication (organizational Users)	Enterprises should ensure that identification and requirements are defined and applied for enterprise users accessing an ICT/OT system or supply chain network. An enterprise user may include employees, individuals deemed to have the equivalent status of employees (e.g., contractors, guest researchers, etc.), and system integrators fulfilling contractor roles. Criteria such as "duration in role" can aid in defining which identification and authentication mechanisms are used. The enterprise may choose to define a set of roles and associate a level of authorization to ensure proper implementation. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Equal	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	10	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.
IA-3	Device Identification and Authentication	Enterprises should implement capabilities to distinctly and positively identify devices and software within their supply chain and, once identified, verify that the identity is authentic. Devices that require unique device-to-device identification and authentication should be defined by type, device, or a combination of type and device. Software that requires authentication should be identified through a software identification tag (SWID) that enables verification of the software package and authentication of the enterprise releasing the software package.	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5	Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.
IA-4(6)	Identifier Management | Cross-organization Management	This enhancement helps the traceability and provenance of elements within the supply chain through the coordination of identifier management among the enterprise and its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. This includes information systems and components as well as individuals engaged in supply chain activities.	Functional	Equal	Cross-Organization Management	IAC-09.4	Mechanisms exist to coordinate username identifiers with external organizations for cross-organization management of identifiers.	10	Coordinate with the following external organizations for cross-organization management of identifiers: [Assignment: organization-defined external organizations].
IR-1	Policy and Procedures	covered procurement, or covered article exists. In such instances, the executive agency shall provide the FASC with relevant information concerning the source or covered article, including 1) the supply chain risk information identified through the course of the agency's activities in furtherance of mitigating, identifying, or managing its supply chain risk and 2) the supply chain risk information regarding covered procurement actions by the agency under the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) 41 U.S.C. § 4713; and any orders issued by the agency under 41 U.S.C. § 4713. Bidirectional communication with supply chain partners should be defined in agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IR-1	Policy and Procedures	covered procurement, or covered article exists. In such instances, the executive agency shall provide the FASC with relevant information concerning the source or covered article, including 1) the supply chain risk information identified through the course of the agency's activities in furtherance of mitigating, identifying, or managing its supply chain risk and 2) the supply chain risk information regarding covered procurement actions by the agency under the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) 41 U.S.C. § 4713; and any orders issued by the agency under 41 U.S.C. § 4713. Bidirectional communication with supply chain partners should be defined in agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IR-1	Policy and Procedures	covered procurement, or covered article exists. In such instances, the executive agency shall provide the FASC with relevant information concerning the source or covered article, including 1) the supply chain risk information identified through the course of the agency's activities in furtherance of mitigating, identifying, or managing its supply chain risk and 2) the supply chain risk information regarding covered procurement actions by the agency under the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) 41 U.S.C. § 4713; and any orders issued by the agency under 41 U.S.C. § 4713. Bidirectional communication with supply chain partners should be defined in agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IR-1	Policy and Procedures	covered procurement, or covered article exists. In such instances, the executive agency shall provide the FASC with relevant information concerning the source or covered article, including 1) the supply chain risk information identified through the course of the agency's activities in furtherance of mitigating, identifying, or managing its supply chain risk and 2) the supply chain risk information regarding covered procurement actions by the agency under the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) 41 U.S.C. § 4713; and any orders issued by the agency under 41 U.S.C. § 4713. Bidirectional communication with supply chain partners should be defined in agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IR-1	Policy and Procedures	covered procurement, or covered article exists. In such instances, the executive agency shall provide the FASC with relevant information concerning the source or covered article, including 1) the supply chain risk information identified through the course of the agency's activities in furtherance of mitigating, identifying, or managing its supply chain risk and 2) the supply chain risk information regarding covered procurement actions by the agency under the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) 41 U.S.C. § 4713; and any orders issued by the agency under 41 U.S.C. § 4713. Bidirectional communication with supply chain partners should be defined in agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IR-4(6)	Incident Handling | Insider Threats	This enhancement helps limit exposure of the C-SCRM information systems, networks, and processes to insider threats. Enterprises should ensure that insider threat incident handling capabilities account for the potential of insider threats associated with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers' personnel with access to ICT/OT systems within the authorization boundary.	Functional	Intersects With	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5	Implement an incident handling capability for incidents involving insider threats.
IR-4(7)	Incident Handling | Insider Threats — Intra-organization Coordination	This enhancement helps limit the exposure of C-SCRM information systems, networks, and processes to insider threats. Enterprises should ensure that insider threat coordination includes suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Intersects With	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5	Coordinate an incident handling capability for insider threats that includes the following organizational entities [Assignment: organization-defined entities].
MA-1	Policy and Procedures	upgrades, patches, the frequency of maintenance, replacement parts, and other aspects of system maintenance. Maintenance policies should be defined for both the system and the network. The maintenance policy should reflect controls based on a risk assessment (including criticality analysis), such as remote access, the roles and attributes of maintenance personnel who have access, the frequency of updates, duration of the contract, the logistical path and method used for updates or maintenance, and monitoring and audit mechanisms. The maintenance policy should state which tools are explicitly allowed or not allowed. For example, in the case of software maintenance, the contract should state the source code, test cases, and other item accessibility needed to maintain a system or components.	Functional	Subset Of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
MA-1	Policy and Procedures	upgrades, patches, the frequency of maintenance, replacement parts, and other aspects of system maintenance. Maintenance policies should be defined for both the system and the network. The maintenance policy should reflect controls based on a risk assessment (including criticality analysis), such as remote access, the roles and attributes of maintenance personnel who have access, the frequency of updates, duration of the contract, the logistical path and method used for updates or maintenance, and monitoring and audit mechanisms. The maintenance policy should state which tools are explicitly allowed or not allowed. For example, in the case of software maintenance, the contract should state the source code, test cases, and other item accessibility needed to maintain a system or components.	Functional	Intersects With	Remote Maintenance Notifications	MNT-05.2	Mechanisms exist to require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time).	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
MA-1	Policy and Procedures	upgrades, patches, the frequency of maintenance, replacement parts, and other aspects of system maintenance. Maintenance policies should be defined for both the system and the network. The maintenance policy should reflect controls based on a risk assessment (including criticality analysis), such as remote access, the roles and attributes of maintenance personnel who have access, the frequency of updates, duration of the contract, the logistical path and method used for updates or maintenance, and monitoring and audit mechanisms. The maintenance policy should state which tools are explicitly allowed or not allowed. For example, in the case of software maintenance, the contract should state the source code, test cases, and other item accessibility needed to maintain a system or components.	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
MA-1	Policy and Procedures	upgrades, patches, the frequency of maintenance, replacement parts, and other aspects of system maintenance. Maintenance policies should be defined for both the system and the network. The maintenance policy should reflect controls based on a risk assessment (including criticality analysis), such as remote access, the roles and attributes of maintenance personnel who have access, the frequency of updates, duration of the contract, the logistical path and method used for updates or maintenance, and monitoring and audit mechanisms. The maintenance policy should state which tools are explicitly allowed or not allowed. For example, in the case of software maintenance, the contract should state the source code, test cases, and other item accessibility needed to maintain a system or components.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
MA-1	Policy and Procedures	upgrades, patches, the frequency of maintenance, replacement parts, and other aspects of system maintenance. Maintenance policies should be defined for both the system and the network. The maintenance policy should reflect controls based on a risk assessment (including criticality analysis), such as remote access, the roles and attributes of maintenance personnel who have access, the frequency of updates, duration of the contract, the logistical path and method used for updates or maintenance, and monitoring and audit mechanisms. The maintenance policy should state which tools are explicitly allowed or not allowed. For example, in the case of software maintenance, the contract should state the source code, test cases, and other item accessibility needed to maintain a system or components.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
MP-1	Policy and Procedures	Various documents and information on a variety of physical and electronic media are disseminated throughout the supply chain. This information may contain a variety of sensitive information and intellectual property from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers and should be appropriately protected. Media protection policies and procedures should also address supply chain concerns, including media in the enterprise's supply chain and throughout the SDLC.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] media protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
MP-1	Policy and Procedures	Various documents and information on a variety of physical and electronic media are disseminated throughout the supply chain. This information may contain a variety of sensitive information and intellectual property from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers and should be appropriately protected. Media protection policies and procedures should also address supply chain concerns, including media in the enterprise's supply chain and throughout the SDLC.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] media protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
MP-1	Policy and Procedures	Various documents and information on a variety of physical and electronic media are disseminated throughout the supply chain. This information may contain a variety of sensitive information and intellectual property from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers and should be appropriately protected. Media protection policies and procedures should also address supply chain concerns, including media in the enterprise's supply chain and throughout the SDLC.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] media protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
MP-4	Media Storage	Media storage controls should include C-SCRM activities. Enterprises should specify and include in agreements (e.g., contracting language) media storage requirements (e.g., encryption) for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The enterprise should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Equal	Media Storage	DCH-06	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	10	a. Physically control and securely store [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
MP-5	Media Transport	The enterprise should incorporate C-SCRM activities when media is transported by enterprise or non-enterprise personnel. Some of the techniques to protect media during transport and storage include cryptographic techniques and approved custodian services.	Functional	Equal	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	10	a. Protect and control [Assignment: organization-defined types of system media] during transport outside of controlled areas using [Assignment: organization-defined controls]; b. Maintain accountability for system media during transport outside of controlled areas; c. Document activities associated with the transport of system media; and
PE-1	Policy and Procedures	The enterprise should integrate C-SCRM practices and requirements into their own physical and environmental protection policy and procedures. The degree of protection should be commensurate with the degree of integration. The physical and environmental protection policy should ensure that the physical interfaces of the supply chain have adequate protection and audit for such protection.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
PE-1	Policy and Procedures	The enterprise should integrate C-SCRM practices and requirements into their own physical and environmental protection policy and procedures. The degree of protection should be commensurate with the degree of integration. The physical and environmental protection policy should ensure that the physical interfaces of the supply chain have adequate protection and audit for such protection.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
PE-1	Policy and Procedures	The enterprise should integrate C-SCRM practices and requirements into their own physical and environmental protection policy and procedures. The degree of protection should be commensurate with the degree of integration. The physical and environmental protection policy should ensure that the physical interfaces of the supply chain have adequate protection and audit for such protection.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among

FDE #	FDE Name	Focal Document Element (FDE) Description NIST SP 800-161 R1 Supplemental C-SCRM Guidance	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
PE-6	Monitoring Physical Access	Individuals who physically access the enterprise or external service provider's facilities, data centers, information, or physical asset(s) – including via the supply chain – may be employed by the enterprise's employees, on-site or remotely located contractors, visitors, other third parties (e.g., maintenance personnel under contract with the contractor enterprise), or an individual affiliated with an enterprise in the upstream supply chain. The enterprise should monitor these individuals' activities to reduce cybersecurity risks throughout the supply chain or require monitoring in agreements.	Functional	Equal	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	10	a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents; b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and c. Coordinate results of reviews and investigations
PE-18	Location of System Components	Physical and environmental hazards or disruptions have an impact on the availability of products that are or will be acquired and physically transported to the enterprise's locations. For example, enterprises should incorporate the manufacturing, warehousing, or the distribution location of information system components that are critical for agency operations when planning for alternative suppliers for these components.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	Position system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.
PL-9	Central Management	C-SCRM controls are managed centrally at Level 1 through the CSCRM Strategy and Implementation Plan and at Level 1 and Level 2 through the C-SCRM Policy. The C-SCRM PMO described in Section 2 centrally manages C-SCRM controls at Level 1 and Level. At Level 3, C-SCRM controls are managed on an information system basis though the SSP and/or CSCRM Plan.	Functional	Intersects With	Centralized Management of Security, Compliance & Resilience Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of security, compliance and resilience controls and related processes.	5	Centrally manage [Assignment: organization-defined controls and related processes].
PL-9	Central Management	C-SCRM controls are managed centrally at Level 1 through the CSCRM Strategy and Implementation Plan and at Level 1 and Level 2 through the C-SCRM Policy. The C-SCRM PMO described in Section 2 centrally manages C-SCRM controls at Level 1 and Level. At Level 3, C-SCRM controls are managed on an information system basis though the SSP and/or CSCRM Plan.	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	Centrally manage [Assignment: organization-defined controls and related processes].
PL-9	Central Management	C-SCRM controls are managed centrally at Level 1 through the CSCRM Strategy and Implementation Plan and at Level 1 and Level 2 through the C-SCRM Policy. The C-SCRM PMO described in Section 2 centrally manages C-SCRM controls at Level 1 and Level. At Level 3, C-SCRM controls are managed on an information system basis though the SSP and/or CSCRM Plan.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	Centrally manage [Assignment: organization-defined controls and related processes].
PL-9	Central Management	C-SCRM controls are managed centrally at Level 1 through the CSCRM Strategy and Implementation Plan and at Level 1 and Level 2 through the C-SCRM Policy. The C-SCRM PMO described in Section 2 centrally manages C-SCRM controls at Level 1 and Level. At Level 3, C-SCRM controls are managed on an information system basis though the SSP and/or CSCRM Plan.	Functional	Intersects With	Centralized Management of Antimalware Technologies	END-04.3	Mechanisms exist to centrally-manage antimalware technologies.	5	Centrally manage [Assignment: organization-defined controls and related processes].
PL-9	Central Management	C-SCRM controls are managed centrally at Level 1 through the CSCRM Strategy and Implementation Plan and at Level 1 and Level 2 through the C-SCRM Policy. The C-SCRM PMO described in Section 2 centrally manages C-SCRM controls at Level 1 and Level. At Level 3, C-SCRM controls are managed on an information system basis though the SSP and/or CSCRM Plan.	Functional	Intersects With	Central Management	END-08.1	Mechanisms exist to centrally-manage anti-phishing and spam protection technologies.	5	Centrally manage [Assignment: organization-defined controls and related processes].
PL-9	Central Management	C-SCRM controls are managed centrally at Level 1 through the CSCRM Strategy and Implementation Plan and at Level 1 and Level 2 through the C-SCRM Policy. The C-SCRM PMO described in Section 2 centrally manages C-SCRM controls at Level 1 and Level. At Level 3, C-SCRM controls are managed on an information system basis though the SSP and/or CSCRM Plan.	Functional	Intersects With	Centralized Management of Event Log Content	MON-03.6	Mechanisms exist to centrally manage and update the criteria to be captured in event logs generated by organization-defined system components.	5	Centrally manage [Assignment: organization-defined controls and related processes].
PM-2	Information Security Program Leadership Role	The senior information security officer (e.g., CISO) and senior agency official responsible for acquisition (e.g., Chief Acquisition Officer [CAO] or Senior Procurement Executive [SPE]) have key responsibilities for C-SCRM and the overall cross-enterprise coordination and collaboration with other applicable senior personnel within the enterprise, such as the CIO, the head of facilities/physical security, and the risk executive (function). This coordination should occur regardless of the specific department and agency enterprise structure and specific titles of relevant senior personnel. The coordination could be executed by the C-SCRM PMO or another similar function. Section 2 provides more guidance on C-SCRM roles and responsibilities.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.
PM-3	Information Security and Privacy Resources	implement agency C-SCRM requirements. Section 3 of this document provides guidance on dedicated funding for C-SCRM programs. The enterprise should also integrate CSCRM requirements into major IT investments to ensure that funding is appropriately allocated through the capital planning and investment request process. For example, should an RFID infrastructure be required to enhance C-SCRM to secure and improve the inventory or logistics management efficiency of the enterprise's supply chain, appropriate IT investments would likely be required to ensure successful planning and implementation. Other examples include any investment into the development or test environment for critical components. In such cases, funding and resources are needed to acquire and maintain appropriate information systems, networks, and components to meet specific C-SCRM requirements that support	Functional	Equal	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement; b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives,
PM-6	Measures of Performance	Enterprises should use measures of performance to track the implementation, efficiency, effectiveness, and impact of C-SCRM activities. The C-SCRM PMO is responsible for creating C-SCRM measures of performance in collaboration with other applicable stakeholders to include identifying the appropriate audience and decision makers and providing guidance on data collection, analysis, and reporting.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	Develop, monitor, and report on the results of information security and privacy measures of performance.
PM-6	Measures of Performance	Enterprises should use measures of performance to track the implementation, efficiency, effectiveness, and impact of C-SCRM activities. The C-SCRM PMO is responsible for creating C-SCRM measures of performance in collaboration with other applicable stakeholders to include identifying the appropriate audience and decision makers and providing guidance on data collection, analysis, and reporting.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	Develop, monitor, and report on the results of information security and privacy measures of performance.
PM-7	Enterprise Architecture	C-SCRM should be integrated when designing and maintaining enterprise architecture.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5	Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.
PM-8	Critical Infrastructure Plan	C-SCRM should be integrated when developing and maintaining critical infrastructure plan	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.
PM-8	Critical Infrastructure Plan	C-SCRM should be integrated when developing and maintaining critical infrastructure plan	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.
PM-9	Risk Management Strategy	The risk management strategy should address cybersecurity risks throughout the supply chain. Section 2, Appendix C, and Appendix D of this document provide guidance on integrating C-SCRM into the risk management strategy.	Functional	Equal	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	a. Develops a comprehensive strategy to manage: 1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and 2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;
PM-10	Authorization Process	C-SCRM should be integrated when designing and implementing authorization processes.	Functional	Equal	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes; b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Integrate the authorization processes into an
PM-11	Mission and Business Process Definition	The enterprise's mission and business processes should address cybersecurity risks throughout the supply chain. When addressing mission and business process definitions, the enterprise should ensure that C-SCRM activities are incorporated into the support processes for achieving mission success. For example, a system supporting a critical mission function that has been designed and implemented for easy removal and replacement should a component fail may require the use of somewhat unreliable hardware components. A C-SCRM activity may need to be defined to ensure that the supplier makes component spare parts readily available if a replacement is needed.	Functional	Equal	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	10	a. Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes;
PM-12	Insider Threat Program	An insider threat program should include C-SCRM and be tailored for both federal and non-federal agency individuals who have access to agency systems and networks. This control applies to contractors and subcontractors and should be implemented throughout the SDLC.	Functional	Equal	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross-discipline insider threat incident handling team.	10	Implement an insider threat program that includes a cross-discipline insider threat incident handling team.
PM-13	Security and Privacy Workforce	Security and privacy workforce development and improvement should ensure that relevant C-SCRM topics are integrated into the content and initiatives produced by the program. Section 2 provides information on C-SCRM roles and responsibilities. NIST SP 800-161 can be used as a source of topics and activities to include in the security and privacy workforce program.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	Establish a security and privacy workforce development and improvement program.
PM-13	Security and Privacy Workforce	Security and privacy workforce development and improvement should ensure that relevant C-SCRM topics are integrated into the content and initiatives produced by the program. Section 2 provides information on C-SCRM roles and responsibilities. NIST SP 800-161 can be used as a source of topics and activities to include in the security and privacy workforce program.	Functional	Intersects With	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	Establish a security and privacy workforce development and improvement program.
PM-14	Testing, Training, and Monitoring	The enterprise should implement a process to ensure that organizational plans for conducting supply chain risk testing, training, and monitoring activities associated with organizational systems are maintained. The C-SCRM PMO can provide guidance and support on how to integrate C-SCRM into testing, training, and monitoring plans.	Functional	Intersects With	Personal Data (PD) Control Testing, Training & Monitoring	PRI-08	Mechanisms exist to conduct testing, training and monitoring activities for Personal Data (PD) controls.	5	a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems: 1. Are developed and maintained; and 2. Continue to be executed; and b. Review testing, training, and monitoring plans for consistency with the organizational risk
PM-14	Testing, Training, and Monitoring	The enterprise should implement a process to ensure that organizational plans for conducting supply chain risk testing, training, and monitoring activities associated with organizational systems are maintained. The C-SCRM PMO can provide guidance and support on how to integrate C-SCRM into testing, training, and monitoring plans.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems: 1. Are developed and maintained; and 2. Continue to be executed; and b. Review testing, training, and monitoring plans for consistency with the organizational risk
PM-15	Security and Privacy Groups and Associations	Contact with security and privacy groups and associations should include C-SCRM practitioners and those with C-SCRM responsibilities. Acquisition, legal, critical infrastructure, and supply chain groups and associations should be incorporated. The C-SCRM PMO can help identify agency personnel who could benefit from participation, specific groups to participate in, and relevant topics.	Functional	Intersects With	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	Establish and institutionalize contact with selected groups and associations within the security and privacy communities: a. To facilitate ongoing security and privacy education and training for organizational personnel; b. To maintain currency with recommended security and privacy practices, techniques, and technologies; and
PM-15	Security and Privacy Groups and Associations	Contact with security and privacy groups and associations should include C-SCRM practitioners and those with C-SCRM responsibilities. Acquisition, legal, critical infrastructure, and supply chain groups and associations should be incorporated. The C-SCRM PMO can help identify agency personnel who could benefit from participation, specific groups to participate in, and relevant topics.	Functional	Intersects With	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the security, compliance and resilience communities to: (1) Facilitate ongoing cybersecurity and data protection education and training for organizational personnel; (2) Maintain currency with recommended cybersecurity and data protection practices, techniques and technologies; and (3) Share current cybersecurity and/or data protection-related information including threats, vulnerabilities and incidents.	5	Establish and institutionalize contact with selected groups and associations within the security and privacy communities: a. To facilitate ongoing security and privacy education and training for organizational personnel; b. To maintain currency with recommended security and privacy practices, techniques, and technologies; and
PM-16	Threat Awareness Program	A threat awareness program should include threats that emanate from the supply chain. When addressing supply chain threat awareness, knowledge should be shared between stakeholders within the boundaries of the enterprise's information sharing policy. The C-SCRM PMO can help identify C-SCRM stakeholders to include in threat information sharing, as well as potential sources of information for supply chain threats.	Functional	Intersects With	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.
PM-18	Privacy Program Plan	The privacy program plan should include C-SCRM. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtier contractors.	Functional	Equal	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	a. Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency's privacy program, and: 1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program; 2. Provides an overview of the requirements for the privacy program and a description of the privacy

FDE #	FDE Name	Focal Document Element (FDE) Description NIST SP 800-161 R1 Supplemental C-SCRM Guidance	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
PM-19	Privacy Program Leadership Role	The privacy program leadership role should be included as a stakeholder in applicable C-SCRM initiatives and activities.	Functional	Equal	Chief Privacy Officer (CPO)	PRI-01.1	Mechanisms exist to appoints a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement, applicable data privacy requirements and manage data privacy risks through the organization-wide data privacy program.	10	Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.
PM-20	Dissemination of Privacy Program Information	The dissemination of privacy program information should be protected from cybersecurity risks throughout the supply chain.	Functional	Equal	Dissemination of Data Privacy Program Information	PRI-01.3	Mechanisms exist to: (1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role; (2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories; (3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy office(s).	10	Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that: a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy;
PM-21	Accounting of Disclosures	An accounting of disclosures should be protected from cybersecurity risks throughout the supply chain.	Functional	Equal	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by: (1) The organization; and/or (2) Relevant third-parties that their PD was shared with.	10	a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including: 1. Date, nature, and purpose of each disclosure; and 2. Name and address, or other contact information of the individual or organization to which the disclosure was made; b. Retain the accounting of disclosures for the
PM-22	Personally Identifiable Information Quality Management	Personally identifiable information (PII) quality management should take into account and manage cybersecurity risks related to PII throughout the supply chain.	Functional	Intersects With	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	5	Develop and document organization-wide policies and procedures for: a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle; b. Correcting or deleting inaccurate or outdated personally identifiable information;
PM-22	Personally Identifiable Information Quality Management	Personally identifiable information (PII) quality management should take into account and manage cybersecurity risks related to PII throughout the supply chain.	Functional	Intersects With	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.	5	Develop and document organization-wide policies and procedures for: a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle; b. Correcting or deleting inaccurate or outdated personally identifiable information;
PM-23	Data Governance Body	Data governance body is a stakeholder in C-SCRM and should be included in cross-agency collaboration and information sharing of C-SCRM activities and initiatives (e.g., by participating in inter-agency bodies, such as the FASC).	Functional	Intersects With	Data Management Board	PRI-13	Mechanisms exist to establish a written charter for a Data Management Board (DMB) and assigned organization-defined roles to the DMB.	5	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].
PM-23	Data Governance Body	Data governance body is a stakeholder in C-SCRM and should be included in cross-agency collaboration and information sharing of C-SCRM activities and initiatives (e.g., by participating in inter-agency bodies, such as the FASC).	Functional	Intersects With	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	5	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].
PM-23	Data Governance Body	Data governance body is a stakeholder in C-SCRM and should be included in cross-agency collaboration and information sharing of C-SCRM activities and initiatives (e.g., by participating in inter-agency bodies, such as the FASC).	Functional	Intersects With	Data Governance	GOV-10	Mechanisms exist to facilitate data governance to oversee the organization's policies, standards and procedures so that sensitive/regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.	5	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].
PM-28	Risk Framing	C-SCRM should be included in risk framing. Section 2 and Appendix C provide detailed guidance on integrating C-SCRM into risk framing.	Functional	Equal	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	10	a. Identify and document: 1. Assumptions affecting risk assessments, risk responses, and risk monitoring; 2. Constraints affecting risk assessments, risk responses, and risk monitoring; 3. Priorities and trade-offs considered by the organization for managing risk; and 4. Organizational risk tolerance;
PM-29	Risk Management Program Leadership Roles	Risk management program leadership roles should include C-SCRM responsibilities and be included in C-SCRM collaboration across the enterprise. Section 2 and Appendix C provide detailed guidance for C-SCRM roles and responsibilities	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and b. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across
PM-29	Risk Management Program Leadership Roles	Risk management program leadership roles should include C-SCRM responsibilities and be included in C-SCRM collaboration across the enterprise. Section 2 and Appendix C provide detailed guidance for C-SCRM roles and responsibilities	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and b. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across
PM-29	Risk Management Program Leadership Roles	Risk management program leadership roles should include C-SCRM responsibilities and be included in C-SCRM collaboration across the enterprise. Section 2 and Appendix C provide detailed guidance for C-SCRM roles and responsibilities	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and b. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across
PM-30	Supply Chain Risk Management Strategy	The Supply Chain Risk Management Strategy (also known as C-SCRM Strategy) should be complemented with a C-SCRM Implementation Plan that lays out detailed initiatives and activities for the enterprise with timelines and responsible parties. This implementation plan can be a POA&M or be included in a POA&M. Based on the C-SCRM Strategy and Implementation Plan at Level 1, the enterprise should select and document common C- SCRM controls that should address the enterprise, program, and system-specific needs. These controls should be iteratively integrated into the C-SCRM Policy at Level 1 and Level 2, as well as the C-SCRM plan (or SSP if required) at Level 3. See Section 2 and Appendix C for further guidance on risk management.	Functional	Equal	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	10	a. Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services; 1. Implement the supply chain risk management strategy consistently across the organization; and (a) Review and update the supply chain risk
PM-31	Continuous Monitoring Strategy	The continuous monitoring strategy and program should integrate CSCRM controls at Levels 1, 2, and 3 in accordance with the Supply Chain Risk Management Strategy.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include: a. Establishing the following organization-wide metrics to be monitored: [Assignment: organization-defined metrics]; b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment:
PS-1	Policy and Procedures	infrastructure activities. Level 1: Applicable roles include risk executive, CIO, CISO, contracting, logistics, delivery/receiving, acquisition security, and other functions that provide supporting supply chain activities. Level 2: Applicable roles include program executive and individuals (e.g., non-federal employees, including contractors) within the acquirer enterprise who are responsible for program success (e.g., Program Manager and other individuals). Level 3: Applicable roles include system engineers or system security engineers throughout the operational system life cycle from requirements definition, development, test, deployment, maintenance, updates, replacements,	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
PS-1	Policy and Procedures	infrastructure activities. Level 1: Applicable roles include risk executive, CIO, CISO, contracting, logistics, delivery/receiving, acquisition security, and other functions that provide supporting supply chain activities. Level 2: Applicable roles include program executive and individuals (e.g., non-federal employees, including contractors) within the acquirer enterprise who are responsible for program success (e.g., Program Manager and other individuals). Level 3: Applicable roles include system engineers or system security engineers throughout the operational system life cycle from requirements definition, development, test, deployment, maintenance, updates, replacements,	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
PS-1	Policy and Procedures	infrastructure activities. Level 1: Applicable roles include risk executive, CIO, CISO, contracting, logistics, delivery/receiving, acquisition security, and other functions that provide supporting supply chain activities. Level 2: Applicable roles include program executive and individuals (e.g., non-federal employees, including contractors) within the acquirer enterprise who are responsible for program success (e.g., Program Manager and other individuals). Level 3: Applicable roles include system engineers or system security engineers throughout the operational system life cycle from requirements definition, development, test, deployment, maintenance, updates, replacements,	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
PT-1	Policy and Procedures	systems. These policy and procedures should address the purpose, scope, roles, responsibilities, management commitment, coordination among enterprise entities, and privacy compliance to support systems/components within information systems or the supply chain. Policies and procedures need to be in place to ensure that contracts state what PII data will be shared, which contractor personnel may have access to the PII, controls protecting PII, how long it can be kept, and what happens to it at the end of a contract. a. When working with a new supplier, ensure that the agreement includes the most recent set of applicable security	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel identifiable information processing and transparency policy that: (a) Addresses purpose, scope, roles, responsibilities,
PT-1	Policy and Procedures	systems. These policy and procedures should address the purpose, scope, roles, responsibilities, management commitment, coordination among enterprise entities, and privacy compliance to support systems/components within information systems or the supply chain. Policies and procedures need to be in place to ensure that contracts state what PII data will be shared, which contractor personnel may have access to the PII, controls protecting PII, how long it can be kept, and what happens to it at the end of a contract. a. When working with a new supplier, ensure that the agreement includes the most recent set of applicable security	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel identifiable information processing and transparency policy that: (a) Addresses purpose, scope, roles, responsibilities,
PT-1	Policy and Procedures	systems. These policy and procedures should address the purpose, scope, roles, responsibilities, management commitment, coordination among enterprise entities, and privacy compliance to support systems/components within information systems or the supply chain. Policies and procedures need to be in place to ensure that contracts state what PII data will be shared, which contractor personnel may have access to the PII, controls protecting PII, how long it can be kept, and what happens to it at the end of a contract. a. When working with a new supplier, ensure that the agreement includes the most recent set of applicable security	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel identifiable information processing and transparency policy that: (a) Addresses purpose, scope, roles, responsibilities,
RA-1	Policy and Procedures	risk assessment should include both the supply chain infrastructure (e.g., development and testing environments and delivery systems) and the information system/components traversing the supply chain. System-level risk assessments significantly intersect with the SDLC and should complement the enterprise's broader RMF activities, which take part during the SDLC. A criticality analysis will ensure that mission-critical functions and components are given higher priority due to their impact on the mission, if compromised. The policy should include supply chainrelevant cybersecurity roles that are applicable to performing and coordinating risk assessments across the enterprise (see Section 2 for the listing and description of roles). Applicable roles within suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers should be	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
RA-1	Policy and Procedures	risk assessment should include both the supply chain infrastructure (e.g., development and testing environments and delivery systems) and the information system/components traversing the supply chain. System-level risk assessments significantly intersect with the SDLC and should complement the enterprise's broader RMF activities, which take part during the SDLC. A criticality analysis will ensure that mission-critical functions and components are given higher priority due to their impact on the mission, if compromised. The policy should include supply chainrelevant cybersecurity roles that are applicable to performing and coordinating risk assessments across the enterprise (see Section 2 for the listing and description of roles). Applicable roles within suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers should be	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
RA-1	Policy and Procedures	risk assessment should include both the supply chain infrastructure (e.g., development and testing environments and delivery systems) and the information system/components traversing the supply chain. System-level risk assessments significantly intersect with the SDLC and should complement the enterprise's broader RMF activities, which take part during the SDLC. A criticality analysis will ensure that mission-critical functions and components are given higher priority due to their impact on the mission, if compromised. The policy should include supply chainrelevant cybersecurity roles that are applicable to performing and coordinating risk assessments across the enterprise (see Section 2 for the listing and description of roles). Applicable roles within suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers should be	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
RA-2	Security Categorization	Security categorization is critical to C-SCRM at Levels 1, 2, and 3. In addition to [FIPS 199] categorization, security categorization for C-SCRM should be based on the criticality analysis that is performed as part of the SDLC. See Section 2 and [NISTIR 8179] for a detailed description of criticality analysis.	Functional	Equal	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	10	a. Categorize the system and information it processes, stores, and transmits; b. Document the security categorization results, including supporting rationale, in the security plan for the system; and c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.
RA-3	Risk Assessment	Risk assessments should include an analysis of criticality, threats, vulnerabilities, likelihood, and impact, as described in detail in Appendix C. The data to be reviewed and collected includes C-SCRM-specific roles, processes, and the results of system/component and services acquisitions, implementation, and integration. Risk assessments should be performed at Levels 1, 2, and 3. Risk assessments at higher levels should consist primarily of a synthesis of various risk assessments performed at lower levels and used for understanding the overall impact with the level (e.g., at the enterprise or mission/function levels). C-SCRM risk assessments should complement and inform risk assessments, which are performed as ongoing activities throughout the SDLC, and processes should be appropriately aligned with or integrated into ERM processes and governance.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	a. Conduct a risk assessment, including: 1. Identifying threats to and vulnerabilities in the system; 2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
RA-3	Risk Assessment	Risk assessments should include an analysis of criticality, threats, vulnerabilities, likelihood, and impact, as described in detail in Appendix C. The data to be reviewed and collected includes C-SCRM-specific roles, processes, and the results of system/component and services acquisitions, implementation, and integration. Risk assessments should be performed at Levels 1, 2, and 3. Risk assessments at higher levels should consist primarily of a synthesis of various risk assessments performed at lower levels and used for understanding the overall impact with the level (e.g., at the enterprise or mission/function levels). C-SCRM risk assessments should complement and inform risk assessments, which are performed as ongoing activities throughout the SDLC, and processes should be appropriately aligned with or integrated into ERM processes and governance.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	a. Conduct a risk assessment, including: 1. Identifying threats to and vulnerabilities in the system; 2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
RA-3(1)	Risk Assessment | Supply Chain Risk Assessment	a. Assess supply chain risks associated with [Assignment: organization-defined systems, system components, and system services]; andb. Update the supply chain risk assessment [Assignment: organization-defined frequency], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.	Functional	Equal	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	10	

FDE #	FDE Name	Focal Document Element (FDE) Description NIST SP 800-161 R1 Supplemental C-SCRM Guidance	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
RA-7	Risk Response	Enterprises should integrate capabilities to respond to cybersecurity risks throughout the supply chain into the enterprise's overall response posture, ensuring that these responses are aligned to and fall within the boundaries of the enterprise's tolerance for risk. Risk response should include consideration of risk response identification, evaluation of alternatives, and risk response decision activities	Functional	Equal	Risk Response	RSK-06.1	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments; (2) Audits; and/or (3) Incidents.	10	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.
RA-9	Criticality Analysis	chain risk management activities. First, enterprises should complete a criticality analysis as part of the Frame step of the C-SCRM Risk Management Process. Then, findings generated in the Assess step activities (e.g., criticality analysis, threat analysis, vulnerability analysis, and mitigation strategies) update and tailor the criticality analysis. A symbiotic relationship exists between the criticality analysis and other Assess step activities in that they inform and enhance one another. For a high-quality criticality analysis, enterprises should employ it iteratively throughout the SLDC and concurrently across the three levels. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should also refer to Appendix F to supplement this guidance in accordance with Executive Order 14028, Improving the	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].
RA-9	Criticality Analysis	chain risk management activities. First, enterprises should complete a criticality analysis as part of the Frame step of the C-SCRM Risk Management Process. Then, findings generated in the Assess step activities (e.g., criticality analysis, threat analysis, vulnerability analysis, and mitigation strategies) update and tailor the criticality analysis. A symbiotic relationship exists between the criticality analysis and other Assess step activities in that they inform and enhance one another. For a high-quality criticality analysis, enterprises should employ it iteratively throughout the SLDC and concurrently across the three levels. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should also refer to Appendix F to supplement this guidance in accordance with Executive Order 14028, Improving the	Functional	Intersects With	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5	Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].
RA-9	Criticality Analysis	chain risk management activities. First, enterprises should complete a criticality analysis as part of the Frame step of the C-SCRM Risk Management Process. Then, findings generated in the Assess step activities (e.g., criticality analysis, threat analysis, vulnerability analysis, and mitigation strategies) update and tailor the criticality analysis. A symbiotic relationship exists between the criticality analysis and other Assess step activities in that they inform and enhance one another. For a high-quality criticality analysis, enterprises should employ it iteratively throughout the SLDC and concurrently across the three levels. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should also refer to Appendix F to supplement this guidance in accordance with Executive Order 14028, Improving the	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].
RA-10	Threat Hunting	functions within the enterprise. Threat hunting capabilities may also be provided via a shared services enterprise, especially when an enterprise lacks the resources to perform threat hunting activities themselves. Typical activities include information sharing with peer enterprises and actively consuming threat intelligence sources (e.g., like those available from Information Assurance and Analysis Centers [ISAC] and Information Assurance and Analysis Organizations [ISAO]). These activities can help identify and flag indicators of increased cybersecurity risks throughout the supply chain that may be of concern, such as cyber incidents, mergers and acquisitions, and Foreign Ownership, Control, or Influence (FOCI). Supply chain threat intelligence should seek out threats to the enterprise's	Functional	Equal	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	10	a. Establish and maintain a cyber threat hunting capability to: 1. Search for indicators of compromise in organizational systems; and 2. Detect, track, and disrupt threats that evade existing controls; and b. Employ the threat hunting capability [Assignment: organization-defined frequency].
SA-1	Policy and Procedures	considered for any and all procurements of products or services in which there may be an unacceptable risk of a supplied product or service contractor compromising the integrity, availability, or confidentiality of an enterprise's information. This initial assessment should occur during the acquisition planning phase and will be minimally informed by an identification and understanding of the criticality of the enterprise's mission functions, its high value assets, and the sensitivity of the information that may be accessible by the supplied product or service provider. In addition, enterprises should develop policies and procedures that address supply chain risks that may arise during contract performance, such as a change of ownership or control of the business or when actionable information is learned that indicates that a supplier or a product is a target of a supply chain threat. Supply chains	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
SA-1	Policy and Procedures	considered for any and all procurements of products or services in which there may be an unacceptable risk of a supplied product or service contractor compromising the integrity, availability, or confidentiality of an enterprise's information. This initial assessment should occur during the acquisition planning phase and will be minimally informed by an identification and understanding of the criticality of the enterprise's mission functions, its high value assets, and the sensitivity of the information that may be accessible by the supplied product or service provider. In addition, enterprises should develop policies and procedures that address supply chain risks that may arise during contract performance, such as a change of ownership or control of the business or when actionable information is learned that indicates that a supplier or a product is a target of a supply chain threat. Supply chains	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
SA-1	Policy and Procedures	considered for any and all procurements of products or services in which there may be an unacceptable risk of a supplied product or service contractor compromising the integrity, availability, or confidentiality of an enterprise's information. This initial assessment should occur during the acquisition planning phase and will be minimally informed by an identification and understanding of the criticality of the enterprise's mission functions, its high value assets, and the sensitivity of the information that may be accessible by the supplied product or service provider. In addition, enterprises should develop policies and procedures that address supply chain risks that may arise during contract performance, such as a change of ownership or control of the business or when actionable information is learned that indicates that a supplier or a product is a target of a supply chain threat. Supply chains	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
SA-2	Allocation of Resources	The enterprise should incorporate C-SCRM requirements when determining and establishing the allocation of resources.	Functional	Equal	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	10	a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning; b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and c. Establish a discrete line item for information
SA-3	System Development Life Cycle	There is a strong relationship between the SDLC and C-SCRM activities. The enterprise should ensure that C-SCRM activities are integrated into the SDLC for both the enterprise and for applicable suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. In addition to traditional SDLC activities, such as requirements and design, the SDLC includes activities such as inventory management, acquisition and procurement, and the logical delivery of systems and components. See Section 2 and Appendix C for further guidance on SDLC. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5	a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations; b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle; c. Identify individuals having information security
SA-3	System Development Life Cycle	There is a strong relationship between the SDLC and C-SCRM activities. The enterprise should ensure that C-SCRM activities are integrated into the SDLC for both the enterprise and for applicable suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. In addition to traditional SDLC activities, such as requirements and design, the SDLC includes activities such as inventory management, acquisition and procurement, and the logical delivery of systems and components. See Section 2 and Appendix C for further guidance on SDLC. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations; b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle; c. Identify individuals having information security
SA-4	Acquisition Process	development methods, techniques, or practices that may be relevant. Identify and specify C-SCRM evaluation criteria, to include the weighting of such criteria. 2. Enterprises should: a. Establish a plan for the acquisition of spare parts to ensure adequate supply, and execute the plan if or when applicable; b. Establish a plan for the acquisition of alternative sources of supply as may be necessary during continuity events or if/when a disruption to the supply chain occurs; c. Work with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service: a. Security and privacy functional requirements; b. Strength of mechanism requirements;
SA-4	Acquisition Process	development methods, techniques, or practices that may be relevant. Identify and specify C-SCRM evaluation criteria, to include the weighting of such criteria. 2. Enterprises should: a. Establish a plan for the acquisition of spare parts to ensure adequate supply, and execute the plan if or when applicable; b. Establish a plan for the acquisition of alternative sources of supply as may be necessary during continuity events or if/when a disruption to the supply chain occurs; c. Work with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service: a. Security and privacy functional requirements; b. Strength of mechanism requirements;
SA-4	Acquisition Process	development methods, techniques, or practices that may be relevant. Identify and specify C-SCRM evaluation criteria, to include the weighting of such criteria. 2. Enterprises should: a. Establish a plan for the acquisition of spare parts to ensure adequate supply, and execute the plan if or when applicable; b. Establish a plan for the acquisition of alternative sources of supply as may be necessary during continuity events or if/when a disruption to the supply chain occurs; c. Work with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service: a. Security and privacy functional requirements; b. Strength of mechanism requirements;
SA-4	Acquisition Process	development methods, techniques, or practices that may be relevant. Identify and specify C-SCRM evaluation criteria, to include the weighting of such criteria. 2. Enterprises should: a. Establish a plan for the acquisition of spare parts to ensure adequate supply, and execute the plan if or when applicable; b. Establish a plan for the acquisition of alternative sources of supply as may be necessary during continuity events or if/when a disruption to the supply chain occurs; c. Work with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	5	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service: a. Security and privacy functional requirements; b. Strength of mechanism requirements;
SA-8	Security and Privacy Engineering Principles	determined by risk assessments (see Section 2 and Appendix C). c. Document and gain management acceptance and approval for risk that is not fully mitigated. d. Limit the number, size, and privilege levels of critical elements. Using criticality analysis will aid in determining which elements or functions are critical. See criticality analysis in Appendix C and NISTIR 8179, Criticality Analysis Process Model: Prioritizing Systems and Components. e. Use security mechanisms that help to reduce opportunities to exploit supply chain cybersecurity vulnerabilities, such as encryption, access control, identity management, and malware or tampering discovery. f. Design information system components and elements to be difficult to disable (e.g., tamperproofing techniques),	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].
SA-8	Security and Privacy Engineering Principles	determined by risk assessments (see Section 2 and Appendix C). c. Document and gain management acceptance and approval for risk that is not fully mitigated. d. Limit the number, size, and privilege levels of critical elements. Using criticality analysis will aid in determining which elements or functions are critical. See criticality analysis in Appendix C and NISTIR 8179, Criticality Analysis Process Model: Prioritizing Systems and Components. e. Use security mechanisms that help to reduce opportunities to exploit supply chain cybersecurity vulnerabilities, such as encryption, access control, identity management, and malware or tampering discovery. f. Design information system components and elements to be difficult to disable (e.g., tamperproofing techniques),	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].
SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	d. Enterprise data and information integrity, confidentiality, and availability requirements are defined and shared with the system suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers as appropriate. e. The consequences of non-compliance with C-SCRM requirements and information system security requirements are defined and documented. f. There is a clear delineation of accountabilities, roles, and responsibilities between contractors when multiple disparate providers are engaged in supporting a system or mission and business function.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].
SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	d. Enterprise data and information integrity, confidentiality, and availability requirements are defined and shared with the system suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers as appropriate. e. The consequences of non-compliance with C-SCRM requirements and information system security requirements are defined and documented. f. There is a clear delineation of accountabilities, roles, and responsibilities between contractors when multiple disparate providers are engaged in supporting a system or mission and business function.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].
SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	d. Enterprise data and information integrity, confidentiality, and availability requirements are defined and shared with the system suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers as appropriate. e. The consequences of non-compliance with C-SCRM requirements and information system security requirements are defined and documented. f. There is a clear delineation of accountabilities, roles, and responsibilities between contractors when multiple disparate providers are engaged in supporting a system or mission and business function.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].
SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	d. Enterprise data and information integrity, confidentiality, and availability requirements are defined and shared with the system suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers as appropriate. e. The consequences of non-compliance with C-SCRM requirements and information system security requirements are defined and documented. f. There is a clear delineation of accountabilities, roles, and responsibilities between contractors when multiple disparate providers are engaged in supporting a system or mission and business function.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].
SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	d. Enterprise data and information integrity, confidentiality, and availability requirements are defined and shared with the system suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers as appropriate. e. The consequences of non-compliance with C-SCRM requirements and information system security requirements are defined and documented. f. There is a clear delineation of accountabilities, roles, and responsibilities between contractors when multiple disparate providers are engaged in supporting a system or mission and business function.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].
SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	d. Enterprise data and information integrity, confidentiality, and availability requirements are defined and shared with the system suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers as appropriate. e. The consequences of non-compliance with C-SCRM requirements and information system security requirements are defined and documented. f. There is a clear delineation of accountabilities, roles, and responsibilities between contractors when multiple disparate providers are engaged in supporting a system or mission and business function.	Functional	Intersects With	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	5	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].
SA-11	Developer Testing and Evaluation	determine whether the supplier (OEM) has performed such testing as part of their quality or security processes. When the acquirer has control over the application and development processes, they should require this testing as part of the SDLC. In addition to the specific types of testing activities described below, enhancements, examples of C-SCRM-relevant testing include testing for counterfeits, verifying the origins of components, examining configuration settings prior to integration, and testing interfaces. These types of tests may require significant resources and should be prioritized based on criticality, threat, and vulnerability analyses (described in Section 2 and Appendix C), as well as the effectiveness of testing techniques. Enterprises may also require third-party testing	Functional	Equal	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	10	Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to: a. Develop and implement a plan for ongoing security and privacy control assessments; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at
SC-1	Policy and Procedures	System and communications protection policies and procedures should address cybersecurity risks throughout the supply chain in relation to the enterprise's processes, systems, and networks. Enterprise-level and program-specific policies help establish and clarify these requirements, and corresponding procedures provide instructions for meeting these requirements. Policies and procedures should include the coordination of communications among and across multiple enterprise entities within the enterprise, as well as the communications methods, external connections, and processes used between the enterprise and its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
SC-1	Policy and Procedures	System and communications protection policies and procedures should address cybersecurity risks throughout the supply chain in relation to the enterprise's processes, systems, and networks. Enterprise-level and program-specific policies help establish and clarify these requirements, and corresponding procedures provide instructions for meeting these requirements. Policies and procedures should include the coordination of communications among and across multiple enterprise entities within the enterprise, as well as the communications methods, external connections, and processes used between the enterprise and its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
SC-1	Policy and Procedures	System and communications protection policies and procedures should address cybersecurity risks throughout the supply chain in relation to the enterprise's processes, systems, and networks. Enterprise-level and program-specific policies help establish and clarify these requirements, and corresponding procedures provide instructions for meeting these requirements. Policies and procedures should include the coordination of communications among and across multiple enterprise entities within the enterprise, as well as the communications methods, external connections, and processes used between the enterprise and its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among

FDE #	FDE Name	Focal Document Element (FDE) Description NIST SP 800-161 R1 Supplemental C-SCRM Guidance	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
SC-1	Policy and Procedures	System and communications protection policies and procedures should address cybersecurity risks throughout the supply chain in relation to the enterprise's processes, systems, and networks. Enterprise-level and program-specific policies help establish and clarify these requirements, and corresponding procedures provide instructions for meeting these requirements. Policies and procedures should include the coordination of communications among and across multiple enterprise entities within the enterprise, as well as the communications methods, external connections, and processes used between the enterprise and its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
SC-47	Alternate Communications Channels	If necessary and appropriate, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers should be included in the alternative communication paths described in this control.	Functional	Equal	Alternate Communications Channels	BCD-10.4	Mechanisms exist to maintain command and control capabilities via alternate communications channels and designating alternative decision makers if primary decision makers are unavailable.	10	Establish [Assignment: organization-defined alternate communications paths] for system operations organizational command and control.
SI-1	Policy and Procedures	The enterprise should include C-SCRM in system and information integrity policy and procedures, including ensuring that program-specific requirements for employing various integrity verification tools and techniques are clearly defined. System and information integrity for information systems, components, and the underlying information systems and networks is critical for managing cybersecurity risks throughout the supply chain. The insertion of malicious code and counterfeits are two primary examples of cybersecurity risks throughout the supply chain, both of which can be at least partially addressed by deploying system and information integrity controls.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
SI-1	Policy and Procedures	The enterprise should include C-SCRM in system and information integrity policy and procedures, including ensuring that program-specific requirements for employing various integrity verification tools and techniques are clearly defined. System and information integrity for information systems, components, and the underlying information systems and networks is critical for managing cybersecurity risks throughout the supply chain. The insertion of malicious code and counterfeits are two primary examples of cybersecurity risks throughout the supply chain, both of which can be at least partially addressed by deploying system and information integrity controls.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
SI-1	Policy and Procedures	The enterprise should include C-SCRM in system and information integrity policy and procedures, including ensuring that program-specific requirements for employing various integrity verification tools and techniques are clearly defined. System and information integrity for information systems, components, and the underlying information systems and networks is critical for managing cybersecurity risks throughout the supply chain. The insertion of malicious code and counterfeits are two primary examples of cybersecurity risks throughout the supply chain, both of which can be at least partially addressed by deploying system and information integrity controls.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
SI-4	System Monitoring	This control includes monitoring vulnerabilities that result from past supply chain cybersecurity compromises, such as malicious code implanted during software development and set to activate after deployment. System monitoring is frequently performed by external service providers. Service-level agreements with these providers should be structured to appropriately reflect this control. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through
SI-4	System Monitoring	This control includes monitoring vulnerabilities that result from past supply chain cybersecurity compromises, such as malicious code implanted during software development and set to activate after deployment. System monitoring is frequently performed by external service providers. Service-level agreements with these providers should be structured to appropriately reflect this control. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through
SI-4	System Monitoring	This control includes monitoring vulnerabilities that result from past supply chain cybersecurity compromises, such as malicious code implanted during software development and set to activate after deployment. System monitoring is frequently performed by external service providers. Service-level agreements with these providers should be structured to appropriately reflect this control. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through
SI-4	System Monitoring	This control includes monitoring vulnerabilities that result from past supply chain cybersecurity compromises, such as malicious code implanted during software development and set to activate after deployment. System monitoring is frequently performed by external service providers. Service-level agreements with these providers should be structured to appropriately reflect this control. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through
SI-5	Security Alerts, Advisories, and Directives	[illegible] follow up if needed. US-CERT, FASC, and other authoritative entities generate security alerts and advisories that are applicable to C-SCRM. Additional laws and regulations will impact who and how additional advisories are provided. Enterprises should ensure that their information-sharing protocols and processes include sharing alerts, advisories, and directives with relevant parties with whom they have an agreement to deliver products or perform services. Enterprises should provide direction or guidance as to what actions are to be taken in response to sharing such an alert, advisory, or directive. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to [illegible]	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generate internal security alerts, advisories, and directives as deemed necessary; c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles];
SI-5	Security Alerts, Advisories, and Directives	follow up if needed. US-CERT, FASC, and other authoritative entities generate security alerts and advisories that are applicable to C-SCRM. Additional laws and regulations will impact who and how additional advisories are provided. Enterprises should ensure that their information-sharing protocols and processes include sharing alerts, advisories, and directives with relevant parties with whom they have an agreement to deliver products or perform services. Enterprises should provide direction or guidance as to what actions are to be taken in response to sharing such an alert, advisory, or directive. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to [illegible]	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generate internal security alerts, advisories, and directives as deemed necessary; c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles];
SI-5	Security Alerts, Advisories, and Directives	follow up if needed. US-CERT, FASC, and other authoritative entities generate security alerts and advisories that are applicable to C-SCRM. Additional laws and regulations will impact who and how additional advisories are provided. Enterprises should ensure that their information-sharing protocols and processes include sharing alerts, advisories, and directives with relevant parties with whom they have an agreement to deliver products or perform services. Enterprises should provide direction or guidance as to what actions are to be taken in response to sharing such an alert, advisory, or directive. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to [illegible]	Functional	Intersects With	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generate internal security alerts, advisories, and directives as deemed necessary; c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles];
SR-1	Policy and Procedures	C-SCRM policies are developed at Level 1 for the overall enterprise and at Level 2 for specific missions and functions. C-SCRM policies can be implemented at Levels 1, 2, and 3, depending on the level of depth and detail. C-SCRM procedures are developed at Level 2 for specific missions and functions and at Level 3 for specific systems. Enterprise functions including but not limited to information security, legal, risk management, and acquisition should review and concur on the development of C-SCRM policies and procedures or provide guidance to system owners for developing system-specific C-SCRM procedures.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] supply chain risk management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
SR-1	Policy and Procedures	C-SCRM policies are developed at Level 1 for the overall enterprise and at Level 2 for specific missions and functions. C-SCRM policies can be implemented at Levels 1, 2, and 3, depending on the level of depth and detail. C-SCRM procedures are developed at Level 2 for specific missions and functions and at Level 3 for specific systems. Enterprise functions including but not limited to information security, legal, risk management, and acquisition should review and concur on the development of C-SCRM policies and procedures or provide guidance to system owners for developing system-specific C-SCRM procedures.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] supply chain risk management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
SR-1	Policy and Procedures	C-SCRM policies are developed at Level 1 for the overall enterprise and at Level 2 for specific missions and functions. C-SCRM policies can be implemented at Levels 1, 2, and 3, depending on the level of depth and detail. C-SCRM procedures are developed at Level 2 for specific missions and functions and at Level 3 for specific systems. Enterprise functions including but not limited to information security, legal, risk management, and acquisition should review and concur on the development of C-SCRM policies and procedures or provide guidance to system owners for developing system-specific C-SCRM procedures.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] supply chain risk management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
SR-3	Supply Chain Controls and Processes	Section 2 and Appendix C of this document provide detailed guidance on implementing this control. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity.	Functional	Equal	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	10	a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel]; b. Employ the following controls to protect against supply chain risks to the system, system
SR-5	Acquisition Strategies, Tools, and Methods	Section 3 and SA controls provide additional guidance on acquisition strategies, tools, and methods. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity.	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	5	Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods].
SR-11	Component Authenticity	[illegible] information technology, IT security, legal, and the C-SCRM PMO. The policy and procedures should address regulatory compliance requirements, contract requirements or clauses, and counterfeit reporting processes to enterprises, such as GIDEP and/or other appropriate enterprises. Where applicable and appropriate, the policy should also address the development and use of a qualified bidders list (QBL) and/or qualified manufacturers list (QML). This helps prevent counterfeits through the use of authorized suppliers, wherever possible, and their integration into the organization's supply chain [CISA SCRM WG3]. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's [illegible]	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5	a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and b. Report counterfeit system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: