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-flowdown.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 controls 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 controls 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 controls 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-2	Account Management	choose to define a set of roles and associate a level of authorization to ensure proper implementation. Enterprises must ensure that accounts for contractor personnel do not exceed the period of performance of the contract. Privileged accounts should only be established for appropriately vetted contractor personnel. Enterprises should also have processes in place to establish and manage temporary or emergency accounts for contractor personnel that require access to a mission-critical or mission-enabling system during a continuity or emergency event. For example, during a pandemic event, existing contractor personnel who are not able to work due to illness may need to be temporarily backfilled by new contractor staff. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies	Functional	Intersects With	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify:
AC-2	Account Management	choose to define a set of roles and associate a level of authorization to ensure proper implementation. Enterprises must ensure that accounts for contractor personnel do not exceed the period of performance of the contract. Privileged accounts should only be established for appropriately vetted contractor personnel. Enterprises should also have processes in place to establish and manage temporary or emergency accounts for contractor personnel that require access to a mission-critical or mission-enabling system during a continuity or emergency event. For example, during a pandemic event, existing contractor personnel who are not able to work due to illness may need to be temporarily backfilled by new contractor staff. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify:
AC-2	Account Management	choose to define a set of roles and associate a level of authorization to ensure proper implementation. Enterprises must ensure that accounts for contractor personnel do not exceed the period of performance of the contract. Privileged accounts should only be established for appropriately vetted contractor personnel. Enterprises should also have processes in place to establish and manage temporary or emergency accounts for contractor personnel that require access to a mission-critical or mission-enabling system during a continuity or emergency event. For example, during a pandemic event, existing contractor personnel who are not able to work due to illness may need to be temporarily backfilled by new contractor staff. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify:
AC-2	Account Management	choose to define a set of roles and associate a level of authorization to ensure proper implementation. Enterprises must ensure that accounts for contractor personnel do not exceed the period of performance of the contract. Privileged accounts should only be established for appropriately vetted contractor personnel. Enterprises should also have processes in place to establish and manage temporary or emergency accounts for contractor personnel that require access to a mission-critical or mission-enabling system during a continuity or emergency event. For example, during a pandemic event, existing contractor personnel who are not able to work due to illness may need to be temporarily backfilled by new contractor staff. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies	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. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify:
AC-3	Access Enforcement	Ensure that the information systems and the supply chain have appropriate access enforcement mechanisms in place. This includes both physical and logical access enforcement mechanisms, which likely work in coordination for supply chain needs. Enterprises should ensure that a defined consequence framework is in place to address access control violations. 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	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
AC-3	Access Enforcement	Ensure that the information systems and the supply chain have appropriate access enforcement mechanisms in place. This includes both physical and logical access enforcement mechanisms, which likely work in coordination for supply chain needs. Enterprises should ensure that a defined consequence framework is in place to address access control violations. 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	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
AC-3	Access Enforcement	Ensure that the information systems and the supply chain have appropriate access enforcement mechanisms in place. This includes both physical and logical access enforcement mechanisms, which likely work in coordination for supply chain needs. Enterprises should ensure that a defined consequence framework is in place to address access control violations. 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	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
AC-4	Information Flow Enforcement	Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Specifying the requirements and how information flow is enforced should ensure that only the required information is communicated to various participants in the supply chain. 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	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	10	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].
AC-5	Separation of Duties	The enterprise should ensure that an appropriate separation of duties is established for decisions that require the acquisition of both information system and supply chain components. The separation of duties helps to ensure that adequate protections are in place for components entering the enterprise's supply chain, such as denying developers the privilege to promote code that they wrote from development to production environments. 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. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and b. Define system access authorizations to support separation of duties.
AC-5	Separation of Duties	The enterprise should ensure that an appropriate separation of duties is established for decisions that require the acquisition of both information system and supply chain components. The separation of duties helps to ensure that adequate protections are in place for components entering the enterprise's supply chain, such as denying developers the privilege to promote code that they wrote from development to production environments. 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	Dual Authorization for Change	CHG-04.3	Mechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or Services (TAAS).	5	a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and b. Define system access authorizations to support separation of duties.
AC-5	Separation of Duties	The enterprise should ensure that an appropriate separation of duties is established for decisions that require the acquisition of both information system and supply chain components. The separation of duties helps to ensure that adequate protections are in place for components entering the enterprise's supply chain, such as denying developers the privilege to promote code that they wrote from development to production environments. 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. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and b. Define system access authorizations to support separation of duties.
AC-5	Separation of Duties	The enterprise should ensure that an appropriate separation of duties is established for decisions that require the acquisition of both information system and supply chain components. The separation of duties helps to ensure that adequate protections are in place for components entering the enterprise's supply chain, such as denying developers the privilege to promote code that they wrote from development to production environments. 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	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and b. Define system access authorizations to support separation of duties.
AC-17	Remote Access	or the operation of information systems, enterprises should implement secure remote access mechanisms and allow remote access only to vetted personnel. Remote access to an enterprise's supply chain (including distributed software development environments) should be limited to the enterprise or contractor personnel and only if and as required to perform their tasks. Remote access requirements – such using a secure VPN, employing multi-factor authentication, or limiting access to specified business hours or from specified geographic locations – must be properly defined in agreements. 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	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize each type of remote 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-23	Data Mining Protection	Enterprises should require their prime contractors to implement this control as part of their insider threat activities and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Data Mining Protection	DCH-16	Mechanisms exist to protect data storage objects against unauthorized data mining and data harvesting techniques.	5	Employ [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to detect and protect against unauthorized data mining.
AC-23	Data Mining Protection	Enterprises should require their prime contractors to implement this control as part of their insider threat activities and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	Employ [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to detect and protect against unauthorized data mining.
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-2(2)	Literacy Training and Awareness | Insider Threat	Enterprises should provide literacy training on recognizing and reporting potential indicators of insider threat within the supply chain. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Equal	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	10	Provide literacy training on recognizing and reporting potential indicators of insider threat.
AT-3	Role-based Training	effectively. Personnel who are part of the acquisition workforce require training on what C-SCRM requirements, clauses, and evaluation factors are necessary to include when conducting procurement and how to incorporate C-SCRM into each acquisition phase. Similar enhanced training requirements should be tailored for personnel responsible for conducting threat assessments. Responding to threats and identified risks requires training in counterintelligence awareness and reporting. Enterprises should ensure that developers receive training on secure development practices as well as the use of vulnerability scanning tools. 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,	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]: 1. Before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; and
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
AU-12	Audit Record Generation	Enterprises should ensure that audit record generation mechanisms are in place to capture all relevant supply chain auditable events. Examples of such events include component version updates, component approvals from acceptance testing results, logistics data-capturing inventory, or transportation information. 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	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5	a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and
AU-13	Monitoring for Information Disclosure	Within the C-SCRM context, information disclosure may occur via multiple avenues, including open source information. For example, supplier-provided errata may reveal information about an enterprise's system that increases the risk to that system. Enterprises should ensure that monitoring is in place for contractor systems to detect the unauthorized disclosure of any data and that contract language includes a requirement that the vendor will notify the enterprise, in accordance with enterprise-defined time frames and as soon as possible in the event of any potential or actual unauthorized disclosure. 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	Monitoring For Information Disclosure	MON-11	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of non-public information.	10	a. Monitor [Assignment: organization-defined open-source information and/or information sites] [Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information; and b. If an information disclosure is discovered: 1. Notify [Assignment: organization-defined personnel or roles]; and
AU-14	Session Audit	Enterprises should include non-federal contract employees in session audits to identify security risks in the supply chain. 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	Session Audit	MON-12	Mechanisms exist to provide session audit capabilities that can: (1) Capture and log all content related to a user session; and (2) Remotely view all content related to an established user session in real time.	10	a. Provide and implement the capability for [Assignment: organization-defined users or roles] to [Selection (one or more): record; view; hear; log] the content of a user session under [Assignment: organization-defined circumstances]; and b. Develop, integrate, and use session auditing activities in consultation with legal counsel and in accordance with applicable laws, executive orders,

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
AU-16(2)	Cross-organizational Audit Logging | Sharing of Audit Information	its system integrators or external services providers, enterprises should establish a set of requirements for the process of sharing audit information. In the case of the system integrator and external service provider and the enterprise, a service-level agreement of the type of audit data required versus what can be provided must be agreed to in advance to ensure that the enterprise obtains the relevant audit information needed to ensure that appropriate protections are in place to meet its mission operation protection needs. Ensure that coverage of both the information systems and supply chain network are addressed for the collection and sharing of audit information. Enterprises should require their prime contractors to implement this control and flow down this requirement to	Functional	Equal	Sharing of Event Logs	MON-14.1	Mechanisms exist to share event logs with third-party organizations based on specific cross-organizational sharing agreements.	10	Provide cross-organizational audit information to [Assignment: organization-defined organizations] based on [Assignment: organization-defined cross-organizational sharing agreements].
CA-3	Information Exchange	with developers, system integrators, external system service providers, other ICT/OT-related service providers, and – in some cases – suppliers. Proper servicelevel agreements should be in place to ensure compliance to system information exchange requirements defined by the enterprise, as the transfer of information between systems in different security or privacy domains with different security or privacy policies introduces the risk that such transfers violate one or more domain security or privacy policies. Examples of such interconnections can include: a. A shared development and operational environment between the enterprise and system integrator b. Product update/patch management connection to an off-the-shelf supplier c. Data request and retrieval transactions in a processing system that resides on an external service provider	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.	5	a. Approve and manage the exchange of information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements;
CM-2	Baseline Configuration	of the baseline is to provide a starting point for tracking changes to components, code, and/or settings throughout the SDLC. Regular reviews and updates of baseline configurations (i.e., re-baselining) are critical for traceability and provenance. The baseline configuration must take into consideration the enterprise's operational environment and any relevant supplier, developer, system integrator, external system service provider, and other ICT/OT-related service provider involvement with the organization's information systems and networks. If the system integrator, for example, uses the existing organization's infrastructure, appropriate measures should be taken to establish a baseline that reflects an appropriate set of agreed-upon criteria for access and operation. Enterprises should require their prime contractors to implement this control and flow down this requirement to	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and b. Review and update the baseline configuration of the system: 1. [Assignment: organization-defined frequency]; 2. When required due to [Assignment: organization-defined circumstances]; and
CM-2	Baseline Configuration	of the baseline is to provide a starting point for tracking changes to components, code, and/or settings throughout the SDLC. Regular reviews and updates of baseline configurations (i.e., re-baselining) are critical for traceability and provenance. The baseline configuration must take into consideration the enterprise's operational environment and any relevant supplier, developer, system integrator, external system service provider, and other ICT/OT-related service provider involvement with the organization's information systems and networks. If the system integrator, for example, uses the existing organization's infrastructure, appropriate measures should be taken to establish a baseline that reflects an appropriate set of agreed-upon criteria for access and operation. Enterprises should require their prime contractors to implement this control and flow down this requirement to	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	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and b. Review and update the baseline configuration of the system: 1. [Assignment: organization-defined frequency]; 2. When required due to [Assignment: organization-defined circumstances]; and
CM-3	Configuration Change Control	Enterprises should determine, implement, monitor, and audit configuration settings and change controls within the information systems and networks and throughout the SDLC. This control supports traceability for C-SCRM. The below NIST SP 800-53, Rev. 5 control enhancements – CM-3 (1), (2), (4), and (8) – are mechanisms that can be used for C-SCRM to collect and manage change control data. 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	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	a. Determine and document the types of changes to the system that are configuration-controlled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; c. Document configuration change decisions associated with the system;
CM-3	Configuration Change Control	Enterprises should determine, implement, monitor, and audit configuration settings and change controls within the information systems and networks and throughout the SDLC. This control supports traceability for C-SCRM. The below NIST SP 800-53, Rev. 5 control enhancements – CM-3 (1), (2), (4), and (8) – are mechanisms that can be used for C-SCRM to collect and manage change control data. 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	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	a. Determine and document the types of changes to the system that are configuration-controlled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; c. Document configuration change decisions associated with the system;
CM-6	Configuration Settings	networks and throughout the SDLC. Methods of oversight include periodic verification, reporting, and review. Resulting information may be shared with various parties that have access to, are connected to, or engage in the creation of the enterprise's information systems and networks on a need-to-know basis. Changes should be tested and approved before they are implemented. Configuration settings should be monitored and audited to alert designated enterprise personnel when a change has occurred. 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	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	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration settings;
CM-6	Configuration Settings	networks and throughout the SDLC. Methods of oversight include periodic verification, reporting, and review. Resulting information may be shared with various parties that have access to, are connected to, or engage in the creation of the enterprise's information systems and networks on a need-to-know basis. Changes should be tested and approved before they are implemented. Configuration settings should be monitored and audited to alert designated enterprise personnel when a change has occurred. 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	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	5	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration settings;
CM-7	Least Functionality	Least functionality reduces the attack surface. Enterprises should select components that allow the flexibility to specify and implement least functionality. Enterprises should ensure least functionality in their information systems and networks and throughout the SDLC. NIST SP 800-53, Rev. 5 control enhancement CM-7 (9) mechanism can be used to protect information systems and networks from vulnerabilities that may be introduced by the use of unauthorized hardware being connected to enterprise systems. 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	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	10	a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].
CM-8	System Component Inventory	numbers, component owners, and for networked components or devices – machine names and network addresses. Inventory specifications may include the manufacturer, device type, model, serial number, and physical location. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtier contractors. Enterprises should specify the requirements and how information flow is enforced to ensure that only the required information – and no more – is communicated to the various participants in the supply chain. If information is subsetted downstream, there should be information about who created the subset information. Enterprises should consider producing SBOMs for applicable and appropriate classes of software,	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and	5	a. Develop and document an inventory of system components that: 1. Accurately reflects the system; 2. Includes all components within the system; 3. Does not include duplicate accounting of components or components assigned to any other system; 4. Is at the level of granularity deemed necessary
CM-8	System Component Inventory	numbers, component owners, and for networked components or devices – machine names and network addresses. Inventory specifications may include the manufacturer, device type, model, serial number, and physical location. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtier contractors. Enterprises should specify the requirements and how information flow is enforced to ensure that only the required information – and no more – is communicated to the various participants in the supply chain. If information is subsetted downstream, there should be information about who created the subset information. Enterprises should consider producing SBOMs for applicable and appropriate classes of software,	Functional	Intersects With	Component Duplication Avoidance	AST-02.3	Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components that prevents assets from being duplicated in other asset inventories.	5	a. Develop and document an inventory of system components that: 1. Accurately reflects the system; 2. Includes all components within the system; 3. Does not include duplicate accounting of components or components assigned to any other system; 4. Is at the level of granularity deemed necessary
CM-9	Configuration Management Plan	Enterprises should ensure that C-SCRM is incorporated into configuration management planning activities. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	Develop, document, and implement a configuration management plan for the system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the
CM-9	Configuration Management Plan	Enterprises should ensure that C-SCRM is incorporated into configuration management planning activities. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5	Develop, document, and implement a configuration management plan for the system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the
CP-2(7)	Contingency Plan | Coordinate with External Service Providers	external service provider have appropriate failover (to include personnel, equipment, and network resources) to reduce or prevent service interruption or ensure timely recovery. Enterprises should ensure that contingency planning requirements are defined as part of the service-level agreement. The agreement may have specific terms that address critical components and functionality support in case of denial-of-service attacks to ensure the continuity of operations. Enterprises should coordinate with external service providers to identify service providers' existing contingency plan practices and build on them as required by the enterprise's mission and business needs. Such coordination will aid in cost reduction and efficient implementation. Enterprises should require their prime contractors who provide a mission- and business-critical or -enabling service or product to implement this control	Functional	Equal	Coordinate With External Service Providers	BCD-01.2	Mechanisms exist to coordinate internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.	10	Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.
CP-3	Contingency Training	Enterprises should ensure that critical suppliers are included in contingency training. 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	Contingency Training	BCD-03	Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.	10	a. Provide contingency training to system users consistent with assigned roles and responsibilities: 1. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility; 2. When required by system changes; and 3. [Assignment: organization-defined frequency] thereafter; and
IA-2	Identification and Authentication (organizational 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	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-4	Identifier Management	system's life within the enterprise. For software development, identifiers should be assigned for those components that have achieved configuration item recognition. For devices and operational systems, identifiers should be assigned when the items enter the enterprise's supply chain, such as when they are transferred to the enterprise's ownership or control through shipping and receiving or via download. Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers typically use their own identifiers for tracking purposes within their own supply chain. Enterprises should correlate those identifiers with the enterprise-assigned identifiers for traceability and accountability. Enterprises	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	Manage system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier; b. Selecting an identifier that identifies an individual, group, role, service, or device; c. Assigning the identifier to the intended individual,
IA-4	Identifier Management	system's life within the enterprise. For software development, identifiers should be assigned for those components that have achieved configuration item recognition. For devices and operational systems, identifiers should be assigned when the items enter the enterprise's supply chain, such as when they are transferred to the enterprise's ownership or control through shipping and receiving or via download. Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers typically use their own identifiers for tracking purposes within their own supply chain. Enterprises should correlate those identifiers with the enterprise-assigned identifiers for traceability and accountability. Enterprises	Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	5	Manage system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier; b. Selecting an identifier that identifies an individual, group, role, service, or device; c. Assigning the identifier to the intended individual,
IA-5	Authenticator Management	This control facilitates traceability and non-repudiation throughout the supply chain. 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	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	Manage system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; b. Establishing initial authenticator content for any authenticators issued by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
IA-5	Authenticator Management	This control facilitates traceability and non-repudiation throughout the supply chain. 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	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	Manage system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; b. Establishing initial authenticator content for any authenticators issued by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
IA-9	Service Identification and Authentication	Enterprises should ensure that identification and authentication are defined and managed for access to services (e.g., web applications using digital certificates, services or applications that query a database as opposed to labor services) throughout the supply chain. Enterprises should ensure that they know what services are being procured and from whom. Services procured should be listed on a validated list of services for the enterprise or have compensating controls in place. 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 Third-Party Technology Assets, Applications and/or Services (TAAS)	IAC-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).	10	Uniquely identify and authenticate [Assignment: organization-defined system services and applications] before establishing communications with devices, users, or other services or applications.
IR-1	Policy and Procedures	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	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	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	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	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-2	Incident Response Training	Enterprises should ensure that critical suppliers are included in incident response training. 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	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	a. Provide incident response training to system users consistent with assigned roles and responsibilities: 1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access; 2. When required by system changes; and 3. [Assignment: organization-defined frequency]
IR-4(10)	Incident Handling | Supply Chain Coordination	providers, other ICT/OT-related service providers, and any relevant interagency bodies to facilitate communications, incident response, root cause, and corrective actions. Enterprises should securely share information through a coordinated set of personnel in key roles to allow for a more comprehensive incident handling approach. Selecting suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers with mature capabilities for supporting supply chain cybersecurity incident handling is important for reducing exposure to cybersecurity risks throughout the supply chain. If transparency for incident handling is limited due to the nature of the relationship, define a set of acceptable criteria in the agreement (e.g., contract). A	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.

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
IR-4(10)	Incident Handling | Supply Chain Coordination	the enterprise may need to coordinate with their suppliers, developers, system integrators, external system service providers, other ICT/OT-related service providers, and any relevant interagency bodies to facilitate communications, incident response, root cause, and corrective actions. Enterprises should securely share information through a coordinated set of personnel in key roles to allow for a more comprehensive incident handling approach. Selecting suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers with mature capabilities for supporting supply chain cybersecurity incident handling is important for reducing exposure to cybersecurity risks throughout the supply chain. If transparency for incident handling is limited due to the nature of the relationship, define a set of acceptable criteria in the agreement (e.g., contract). A	Functional	Intersects With	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for TAAS related to the incident.	5	Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.
IR-6(3)	Incident Reporting | Supply Chain Coordination	Communications of security incident information from the enterprise to suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers and vice versa require protection. The enterprise should ensure that information is reviewed and approved for sending based on its agreements with suppliers and any relevant interagency bodies. Any escalation of or exception from this reporting should be clearly defined in the agreement. The enterprise should ensure that incident reporting data is adequately protected for transmission and received by approved individuals only. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for TAAS related to the incident.	5	Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.
IR-7(2)	Incident Response Assistance | Coordination with External Providers	The enterprise's agreements with prime contractors should specify the conditions under which a government-approved or -designated third party would be available or may be required to provide assistance with incident response, as well as the role and responsibility of that third party.	Functional	Equal	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	10	(a) Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability; and (b) Identify organizational incident response team members to the external providers.
IR-8	Incident Response Plan	Enterprises should coordinate, develop, and implement an incident response plan that includes information-sharing responsibilities with critical suppliers and, in a federal context, interagency partners and the FASC. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Equal	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10	a. Develop an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization;
IR-9	Information Spillage Response	The supply chain is vulnerable to information spillage. The enterprise should include supply chain-related information spills in its information spillage response plan. This may require coordination with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The details of how this coordination is to be conducted should be included in the agreement (e.g., contract). Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive/regulated data spills.	5	Respond to information spills by: a. Assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills; b. Identifying the specific information involved in the system contamination; c. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a
IR-9	Information Spillage Response	The supply chain is vulnerable to information spillage. The enterprise should include supply chain-related information spills in its information spillage response plan. This may require coordination with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The details of how this coordination is to be conducted should be included in the agreement (e.g., contract). Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Sensitive / Regulated Data Spill Responsible Personnel	IRO-12.1	Mechanisms exist to formally assign personnel or roles with responsibility for responding to sensitive/regulated data spills.	5	Respond to information spills by: a. Assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills; b. Identifying the specific information involved in the system contamination; c. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a
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
MA-4	Nonlocal Maintenance	Nonlocal maintenance may be provided by contractor personnel. Appropriate protections should be in place to manage associated risks. Controls applied to internal maintenance personnel are applied to any suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers performing a similar maintenance role and enforced through contractual agreements with their external service providers.	Functional	Intersects With	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	5	a. Approve and monitor nonlocal maintenance and diagnostic activities; b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system; c. Employ strong authentication in the establishment of nonlocal maintenance and
MA-4	Nonlocal Maintenance	Nonlocal maintenance may be provided by contractor personnel. Appropriate protections should be in place to manage associated risks. Controls applied to internal maintenance personnel are applied to any suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers performing a similar maintenance role and enforced through contractual agreements with their external service providers.	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. Approve and monitor nonlocal maintenance and diagnostic activities; b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system; c. Employ strong authentication in the establishment of nonlocal maintenance and
MA-4	Nonlocal Maintenance	Nonlocal maintenance may be provided by contractor personnel. Appropriate protections should be in place to manage associated risks. Controls applied to internal maintenance personnel are applied to any suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers performing a similar maintenance role and enforced through contractual agreements with their external service providers.	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. Approve and monitor nonlocal maintenance and diagnostic activities; b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system; c. Employ strong authentication in the establishment of nonlocal maintenance and
MA-5(4)	Maintenance Personnel | Foreign Nationals	The vetting of foreign nationals with access to critical non-national security systems/services must take C-SCRM into account and be extended to all relevant contractor personnel. Enterprises should specify in agreements any restrictions or vetting requirements that pertain to foreign nationals and flow the requirements down to relevant subcontractors.	Functional	Intersects With	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.	5	Ensure that: (a) Foreign nationals with appropriate security clearances are used to conduct maintenance and diagnostic activities on classified systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and
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-6	Media Sanitization	Enterprises should specify and include in agreements (e.g., contracting language) media sanitization policies for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Media is used throughout the SDLC. Media traversing or residing in the supply chain may originate anywhere, including from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. It can be new, refurbished, or reused. Media sanitization is critical to ensuring that information is removed before the media is used, reused, or discarded. For media that contains privacy or other sensitive information (e.g., CUI), the enterprise should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; and b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the
MP-6	Media Sanitization	Enterprises should specify and include in agreements (e.g., contracting language) media sanitization policies for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Media is used throughout the SDLC. Media traversing or residing in the supply chain may originate anywhere, including from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. It can be new, refurbished, or reused. Media sanitization is critical to ensuring that information is removed before the media is used, reused, or discarded. For media that contains privacy or other sensitive information (e.g., CUI), the enterprise should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; and b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the
MP-6	Media Sanitization	Enterprises should specify and include in agreements (e.g., contracting language) media sanitization policies for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Media is used throughout the SDLC. Media traversing or residing in the supply chain may originate anywhere, including from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. It can be new, refurbished, or reused. Media sanitization is critical to ensuring that information is removed before the media is used, reused, or discarded. For media that contains privacy or other sensitive information (e.g., CUI), the enterprise should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	5	a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; and b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the
PE-2	Physical Access Authorizations	information, systems, or data centers (e.g., sensitive or classified). Such authorizations should specify what the individual is permitted or not permitted to do with regard to their physical access (e.g., view, alter/configure, insert something, connect something, remove, etc.). Agreements should address physical access authorization requirements, and the enterprise should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Authorization for non-federal employees should follow an approved protocol, which includes documentation of the authorization and specifies any prerequisites or constraints that pertain to such authorization (e.g., individual must be escorted by a federal employee, individual must be badged,	Functional	Equal	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	10	a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides; b. Issue authorization credentials for facility access; c. Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and d. Remove individuals from the facility access list
PE-23	Facility Location	suppliers. Factors may include geographic location (e.g., Continental United States [CONUS], Outside the Continental United States [OCONUS]), physical protections in place at one or more of the relevant facilities, local management and control of such facilities, environmental hazard potential (e.g., located in a high-risk seismic zone), and alternative facility locations. Enterprises should also assess whether the location of a manufacturing or distribution center could be influenced by geopolitical, economic, or other factors. For critical vendors or products, enterprises should specifically address any requirements or restrictions concerning the facility locations of the vendors (or their upstream supply chain providers) in contracts and flow down this requirement to relevant sub-	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.
PE-23	Facility Location	suppliers. Factors may include geographic location (e.g., Continental United States [CONUS], Outside the Continental United States [OCONUS]), physical protections in place at one or more of the relevant facilities, local management and control of such facilities, environmental hazard potential (e.g., located in a high-risk seismic zone), and alternative facility locations. Enterprises should also assess whether the location of a manufacturing or distribution center could be influenced by geopolitical, economic, or other factors. For critical vendors or products, enterprises should specifically address any requirements or restrictions concerning the facility locations of the vendors (or their upstream supply chain providers) in contracts and flow down this requirement to relevant sub-	Functional	Intersects With	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	5	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.
PE-23	Facility Location	suppliers. Factors may include geographic location (e.g., Continental United States [CONUS], Outside the Continental United States [OCONUS]), physical protections in place at one or more of the relevant facilities, local management and control of such facilities, environmental hazard potential (e.g., located in a high-risk seismic zone), and alternative facility locations. Enterprises should also assess whether the location of a manufacturing or distribution center could be influenced by geopolitical, economic, or other factors. For critical vendors or products, enterprises should specifically address any requirements or restrictions concerning the facility locations of the vendors (or their upstream supply chain providers) in contracts and flow down this requirement to relevant sub-	Functional	Intersects With	Alternate Storage Site	BCD-08	Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information.	5	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.
PE-23	Facility Location	suppliers. Factors may include geographic location (e.g., Continental United States [CONUS], Outside the Continental United States [OCONUS]), physical protections in place at one or more of the relevant facilities, local management and control of such facilities, environmental hazard potential (e.g., located in a high-risk seismic zone), and alternative facility locations. Enterprises should also assess whether the location of a manufacturing or distribution center could be influenced by geopolitical, economic, or other factors. For critical vendors or products, enterprises should specifically address any requirements or restrictions concerning the facility locations of the vendors (or their upstream supply chain providers) in contracts and flow down this requirement to relevant sub-	Functional	Intersects With	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.	5	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.
PE-23	Facility Location	suppliers. Factors may include geographic location (e.g., Continental United States [CONUS], Outside the Continental United States [OCONUS]), physical protections in place at one or more of the relevant facilities, local management and control of such facilities, environmental hazard potential (e.g., located in a high-risk seismic zone), and alternative facility locations. Enterprises should also assess whether the location of a manufacturing or distribution center could be influenced by geopolitical, economic, or other factors. For critical vendors or products, enterprises should specifically address any requirements or restrictions concerning the facility locations of the vendors (or their upstream supply chain providers) in contracts and flow down this requirement to relevant sub-	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	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.
PE-23	Facility Location	suppliers. Factors may include geographic location (e.g., Continental United States [CONUS], Outside the Continental United States [OCONUS]), physical protections in place at one or more of the relevant facilities, local management and control of such facilities, environmental hazard potential (e.g., located in a high-risk seismic zone), and alternative facility locations. Enterprises should also assess whether the location of a manufacturing or distribution center could be influenced by geopolitical, economic, or other factors. For critical vendors or products, enterprises should specifically address any requirements or restrictions concerning the facility locations of the vendors (or their upstream supply chain providers) in contracts and flow down this requirement to relevant sub-	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.
PL-2	System Security and Privacy Plans	Plan at Level 1 and the C-SCRM policy at Level 1 and Level 2. In addition to internal coordination, the enterprise should coordinate with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to develop and maintain their SSPs. For example, building and operating a system requires a significant coordination and collaboration between the enterprise and system integrator personnel. Such coordination and collaboration should be addressed in the system security plan or stand-alone C-SCRM plan. These plans should also consider that suppliers or external service providers may not be able to customize to the acquirer's requirements. It is recommended that suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers also develop C-SCRM plans for non-federal (i.e., contractor)	Functional	Intersects With	Plan / Coordinate with Other Organizational Entities	IAO-03.1	Mechanisms exist to plan and coordinate Information Assurance Program (IAP) activities with affected stakeholders before conducting such activities in order to reduce the potential impact on operations.	5	a. Develop security and privacy plans for the system that: 1. Are consistent with the organization's enterprise architecture; 2. Explicitly define the constituent system components; 3. Describe the operational context of the system in terms of mission and business processes;
PL-2	System Security and Privacy Plans	Plan at Level 1 and the C-SCRM policy at Level 1 and Level 2. In addition to internal coordination, the enterprise should coordinate with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to develop and maintain their SSPs. For example, building and operating a system requires a significant coordination and collaboration between the enterprise and system integrator personnel. Such coordination and collaboration should be addressed in the system security plan or stand-alone C-SCRM plan. These plans should also consider that suppliers or external service providers may not be able to customize to the acquirer's requirements. It is recommended that suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers also develop C-SCRM plans for non-federal (i.e., contractor)	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes	5	a. Develop security and privacy plans for the system that: 1. Are consistent with the organization's enterprise architecture; 2. Explicitly define the constituent system components; 3. Describe the operational context of the system in terms of mission and business processes;

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
PL-2	System Security and Privacy Plans	Plan at Level 1 and the C-SCRM policy at Level 1 and Level 2. In addition to internal coordination, the enterprise should coordinate with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to develop and maintain their SSPs. For example, building and operating a system requires a significant coordination and collaboration between the enterprise and system integrator personnel. Such coordination and collaboration should be addressed in the system security plan or stand-alone C-SCRM plan. These plans should also consider that suppliers or external service providers may not be able to customize to the acquirer's requirements. It is recommended that suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers also develop C-SCRM plans for non-federal (i.e., contractor)	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5	a. Develop security and privacy plans for the system that: 1. Are consistent with the organization's enterprise architecture; 2. Explicitly define the constituent system components; 3. Describe the operational context of the system in terms of mission and business processes;
PM-5	System Inventory	Having a current system inventory is foundational for C-SCRM. Not having a system inventory may lead to the enterprise's inability to identify system and supplier criticality, which would result in an inability to conduct C-SCRM activities. To ensure that all applicable suppliers are identified and categorized for criticality, enterprises should include relevant supplier information in the system inventory and maintain its currency and accuracy. 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	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.
PM-5	System Inventory	Having a current system inventory is foundational for C-SCRM. Not having a system inventory may lead to the enterprise's inability to identify system and supplier criticality, which would result in an inability to conduct C-SCRM activities. To ensure that all applicable suppliers are identified and categorized for criticality, enterprises should include relevant supplier information in the system inventory and maintain its currency and accuracy. 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	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and	5	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.
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
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
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
PS-3	Personnel Screening	To mitigate insider threat risk, personnel screening policies and procedures should be extended to any contractor personnel with authorized access to information systems, system components, or information system services. Continuous monitoring activities should be commensurate with the contractor's level of access to sensitive, classified, or regulated information and should be consistent with broader enterprise policies. Screening requirements should be incorporated into agreements and flow down to sub-tier contractors	Functional	Equal	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	a. Screen individuals prior to authorizing access to the system; and b. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening].
PS-6	Access Agreements	Additionally, terms of access should be consistent with the enterprise's information security policy and may need to specify additional restrictions, such as allowing access during specific timeframes, from specific locations, or only by personnel who have satisfied additional vetting requirements. The enterprise should deploy audit mechanisms to review, monitor, update, and track access by these parties in accordance with the access agreement. As personnel vary over time, the enterprise should implement a timely and rigorous personnel security update process for the access agreements. When information systems and network products and services are provided by an entity within the enterprise, there may be an existing access agreement in place. When such an agreement does not exist, it should be established.	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	5	a. Develop and document access agreements for organizational systems; b. Review and update the access agreements [Assignment: organization-defined frequency]; and c. Verify that individuals requiring access to organizational information and systems: 1. Sign appropriate access agreements prior to being granted access; and
PS-6	Access Agreements	specify additional restrictions, such as allowing access during specific timeframes, from specific locations, or only by personnel who have satisfied additional vetting requirements. The enterprise should deploy audit mechanisms to review, monitor, update, and track access by these parties in accordance with the access agreement. As personnel vary over time, the enterprise should implement a timely and rigorous personnel security update process for the access agreements. When information systems and network products and services are provided by an entity within the enterprise, there may be an existing access agreement in place. When such an agreement does not exist, it should be established.	Functional	Intersects With	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	5	a. Develop and document access agreements for organizational systems; b. Review and update the access agreements [Assignment: organization-defined frequency]; and c. Verify that individuals requiring access to organizational information and systems: 1. Sign appropriate access agreements prior to being granted access; and
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] personally 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] personally 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] personally identifiable information processing and transparency policy that: (a) Addresses purpose, scope, roles, responsibilities,
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	
RA-5	Vulnerability Monitoring and Scanning	monitoring activities requires enterprises to consider suppliers as well as their sub-suppliers. Enterprises, where applicable and appropriate, may consider providing customers with a Vulnerability Disclosure Report (VDR) to demonstrate proper and complete vulnerability assessments for components listed in SBOMs. The VDR should include the analysis and findings describing the impact (or lack of impact) that the reported vulnerability has on a component or product. The VDR should also contain information on plans to address the CVE. Enterprises should consider publishing the VDR within a secure portal available to customers and signing the VDR with a trusted, verifiable, private key that includes a timestamp indicating the date and time of the VDR signature and associated	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among
RA-5	Vulnerability Monitoring and Scanning	monitoring activities requires enterprises to consider suppliers as well as their sub-suppliers. Enterprises, where applicable and appropriate, may consider providing customers with a Vulnerability Disclosure Report (VDR) to demonstrate proper and complete vulnerability assessments for components listed in SBOMs. The VDR should include the analysis and findings describing the impact (or lack of impact) that the reported vulnerability has on a component or product. The VDR should also contain information on plans to address the CVE. Enterprises should consider publishing the VDR within a secure portal available to customers and signing the VDR with a trusted, verifiable, private key that includes a timestamp indicating the date and time of the VDR signature and associated	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among
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 highquality 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 highquality 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 highquality 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].
SA-21	Developer Screening	The enterprise should implement screening processes for their internal developers. For system integrators who may be providing key developers that address critical components, the enterprise should ensure that appropriate processes for developer screening have been used. The screening of developers should be included as a contractual requirement and be a flow-down requirement to relevant sub-level subcontractors who provide development services or who have access to the development environment.	Functional	Equal	Developer Screening	TDA-13	Mechanisms exist to ensure that the developers of Technology Assets, Applications and/or Services (TAAS) have the requisite skillset and appropriate access authorizations.	10	Require that the developer of [Assignment: organization-defined system, system component, or system service]: a. Has appropriate access authorizations as determined by assigned [Assignment: organization-defined official government duties]; and b. Satisfies the following additional personnel screening criteria: [Assignment: organization-
SC-7	Boundary Protection	agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. There may be multiple interfaces throughout the enterprise, supplier systems and networks, and the SDLC. Appropriate vulnerability, threat, and risk assessments should be performed to ensure proper boundary protections for supply chain components and supply chain information flow. The vulnerability, threat, and risk assessments can aid in scoping boundary protection to a relevant set of criteria and help manage associated costs. For contracts with external service providers, enterprises should ensure that the provider satisfies boundary control requirements pertinent to environments and networks within their span of control. Further detail is provided in Section 2 and Appendix C. Enterprises should require their prime contractors to implement this	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connect to external networks or systems only
SC-7(13)	Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components	The enterprise should provide separation and isolation of development, test, and security assessment tools and operational environments and relevant monitoring tools within the enterprise's information systems and networks. This control applies the entity responsible for creating software and hardware, to include federal agencies and prime contractors. As such, this controls applies to the federal agency and applicable supplier information systems and networks. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. If a compromise or information leakage happens in any one environment, the other environments should still be protected through the separation and isolation mechanisms or techniques.	Functional	Intersects With	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.	5	Isolate [Assignment: organization-defined information security tools, mechanisms, and support components] from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.
SC-8	Transmission Confidentiality and Integrity	Acquirers, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers may repurpose existing security mechanisms (e.g., authentication, authorization, or encryption) to achieve enterprise confidentiality and integrity requirements. The degree of protection should be based on the sensitivity of information to be transmitted and the relationship between the enterprise and the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.
SC-8	Transmission Confidentiality and Integrity	Acquirers, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers may repurpose existing security mechanisms (e.g., authentication, authorization, or encryption) to achieve enterprise confidentiality and integrity requirements. The degree of protection should be based on the sensitivity of information to be transmitted and the relationship between the enterprise and the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.
SC-28	Protection of Information at Rest	suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The enterprise should also ensure that they provide appropriate protections within the information systems and networks for data at rest for the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers information, such as source code, testing data, blueprints, and intellectual property information. This control should be applied throughout the SDLC, including during requirements, development, manufacturing, test, inventory management, maintenance, and disposal. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].
SC-28	Protection of Information at Rest	suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The enterprise should also ensure that they provide appropriate protections within the information systems and networks for data at rest for the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers information, such as source code, testing data, blueprints, and intellectual property information. This control should be applied throughout the SDLC, including during requirements, development, manufacturing, test, inventory management, maintenance, and disposal. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].
SC-36	Distributed Processing and Storage	Processing and storage can be distributed both across the enterprise's systems and networks and across the SDLC. The enterprise should ensure that these techniques are applied in both contexts. Development, manufacturing, configuration management, test, maintenance, and operations can use distributed processing and storage. This control applies to the entity responsible for processing and storage functions or related infrastructure, to include federal agencies and contractors. As such, this control applies to the federal agency and applicable supplier information systems and networks. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Equal	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.	10	Distribute the following processing and storage components across multiple [Selection: physical locations; logical domains]: [Assignment: organization-defined processing and storage components].

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
SI-2	Flaw Remediation	The output of flaw remediation activities provides useful input into the ICT/OT SCRM processes described in Section 2 and Appendix C. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	a. Identify, report, and correct system flaws; b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and d. Incorporate flaw remediation into the
SI-2	Flaw Remediation	The output of flaw remediation activities provides useful input into the ICT/OT SCRM processes described in Section 2 and Appendix C. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	a. Identify, report, and correct system flaws; b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and d. Incorporate flaw remediation into the
SI-2	Flaw Remediation	The output of flaw remediation activities provides useful input into the ICT/OT SCRM processes described in Section 2 and Appendix C. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	a. Identify, report, and correct system flaws; b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and d. Incorporate flaw remediation into the
SI-3	Malicious Code Protection	Because the majority of code operated in federal systems is not developed by the Federal Government, malicious code threats often originate from the supply chain. This controls applies to the federal agency and contractors with code-related responsibilities (e.g., developing code, installing patches, performing system upgrades, etc.), as well as applicable contractor information systems and networks. 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	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;
SI-3	Malicious Code Protection	Because the majority of code operated in federal systems is not developed by the Federal Government, malicious code threats often originate from the supply chain. This controls applies to the federal agency and contractors with code-related responsibilities (e.g., developing code, installing patches, performing system upgrades, etc.), as well as applicable contractor information systems and networks. 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	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;
SI-3	Malicious Code Protection	Because the majority of code operated in federal systems is not developed by the Federal Government, malicious code threats often originate from the supply chain. This controls applies to the federal agency and contractors with code-related responsibilities (e.g., developing code, installing patches, performing system upgrades, etc.), as well as applicable contractor information systems and networks. 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	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;
SI-3	Malicious Code Protection	Because the majority of code operated in federal systems is not developed by the Federal Government, malicious code threats often originate from the supply chain. This controls applies to the federal agency and contractors with code-related responsibilities (e.g., developing code, installing patches, performing system upgrades, etc.), as well as applicable contractor information systems and networks. 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	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;
SI-3	Malicious Code Protection	Because the majority of code operated in federal systems is not developed by the Federal Government, malicious code threats often originate from the supply chain. This controls applies to the federal agency and contractors with code-related responsibilities (e.g., developing code, installing patches, performing system upgrades, etc.), as well as applicable contractor information systems and networks. 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. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;
SI-3	Malicious Code Protection	Because the majority of code operated in federal systems is not developed by the Federal Government, malicious code threats often originate from the supply chain. This controls applies to the federal agency and contractors with code-related responsibilities (e.g., developing code, installing patches, performing system upgrades, etc.), as well as applicable contractor information systems and networks. 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	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;
SI-3	Malicious Code Protection	Because the majority of code operated in federal systems is not developed by the Federal Government, malicious code threats often originate from the supply chain. This controls applies to the federal agency and contractors with code-related responsibilities (e.g., developing code, installing patches, performing system upgrades, etc.), as well as applicable contractor information systems and networks. 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. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;
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	The enterprise should evaluate security alerts, advisories, and directives for cybersecurity supply chain impacts and 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 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. 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	The enterprise should evaluate security alerts, advisories, and directives for cybersecurity supply chain impacts and 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 implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	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	The enterprise should evaluate security alerts, advisories, and directives for cybersecurity supply chain impacts and 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 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. 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-7	Software, Firmware, and Information Integrity	impacted by unanticipated changes. The integrity of systems and components should also be tested and verified. Applicable verification tools include digital signature or checksum verification; acceptance testing for physical components; confining software to limited privilege environments, such as sandboxes; code execution in contained environments prior to use; and ensuring that if only binary or machine-executable code is available, it is obtained directly from the OEM or a verified supplier or distributer. Mechanisms for this control are discussed in detail in [NIST SP 800-53, Rev. 5]. This control applies to federal agencies and applicable supplier information systems and networks. When purchasing an ICT/OT product, an enterprise should perform due diligence to understand what a supplier's integrity assurance practices are. Enterprises should require their prime contractors to implement this	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	5	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; and b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined
SI-7	Software, Firmware, and Information Integrity	impacted by unanticipated changes. The integrity of systems and components should also be tested and verified. Applicable verification tools include digital signature or checksum verification; acceptance testing for physical components; confining software to limited privilege environments, such as sandboxes; code execution in contained environments prior to use; and ensuring that if only binary or machine-executable code is available, it is obtained directly from the OEM or a verified supplier or distributer. Mechanisms for this control are discussed in detail in [NIST SP 800-53, Rev. 5]. This control applies to federal agencies and applicable supplier information systems and networks. When purchasing an ICT/OT product, an enterprise should perform due diligence to understand what a supplier's integrity assurance practices are. Enterprises should require their prime contractors to implement this	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. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; and b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined
SI-7	Software, Firmware, and Information Integrity	impacted by unanticipated changes. The integrity of systems and components should also be tested and verified. Applicable verification tools include digital signature or checksum verification; acceptance testing for physical components; confining software to limited privilege environments, such as sandboxes; code execution in contained environments prior to use; and ensuring that if only binary or machine-executable code is available, it is obtained directly from the OEM or a verified supplier or distributer. Mechanisms for this control are discussed in detail in [NIST SP 800-53, Rev. 5]. This control applies to federal agencies and applicable supplier information systems and networks. When purchasing an ICT/OT product, an enterprise should perform due diligence to understand what a supplier's integrity assurance practices are. Enterprises should require their prime contractors to implement this	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; and b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined
SI-20	Tainting	Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers may have access to the sensitive information of a federal agency. In this instance, enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Equal	Tainting	THR-08	Mechanisms exist to embed false data or steganographic data in files to enable the organization to determine if data has been exfiltrated and provide a means to identify the individual(s) involved.	10	Embed data or capabilities in the following systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization: [Assignment: organization-defined systems or system components].
SR-3(3)	Supply Chain Controls and Processes | Sub-tier Flow Down	to protect the supply chain. As part of procurement requirements, enterprises should include the need for suppliers to flow down controls to subcontractors throughout the SDLC. As part of market research and analysis activities, enterprises should conduct robust due diligence research on potential suppliers or products, as well as their upstream dependencies (e.g., fourth- and fifth-party suppliers), which can help enterprises avoid single points of failure within their supply chains. The results of this research can be helpful in shaping the sourcing approach and refining requirements. An evaluation of the cybersecurity risks that arise from a supplier, product, or service should be completed prior to the contract award decision to ensure that the holistic risk profile is well-understood and serves as a weighted factor in award decisions. During the period of performance, suppliers should be monitored for	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	Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.
SR-3(3)	Supply Chain Controls and Processes | Sub-tier Flow Down	to protect the supply chain. As part of procurement requirements, enterprises should include the need for suppliers to flow down controls to subcontractors throughout the SDLC. As part of market research and analysis activities, enterprises should conduct robust due diligence research on potential suppliers or products, as well as their upstream dependencies (e.g., fourth- and fifth-party suppliers), which can help enterprises avoid single points of failure within their supply chains. The results of this research can be helpful in shaping the sourcing approach and refining requirements. An evaluation of the cybersecurity risks that arise from a supplier, product, or service should be completed prior to the contract award decision to ensure that the holistic risk profile is well-understood and serves as a weighted factor in award decisions. During the period of performance, suppliers should be monitored for	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.
SR-10	Inspection of Systems or Components	controls are in place and to examine whether there is evidence of tampering. Products or components should be inspected prior to use and periodically thereafter. Inspection requirements should also be included in contracts with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors and flow down to subcontractors, when relevant. Criticality analysis can help determine which systems and components are critical and should therefore be subjected to inspection. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis. The C-SCRM PMO can help identify critical systems and components, especially those that are used by multiple missions,	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	Inspect the following systems or system components [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].
SR-10	Inspection of Systems or Components	controls are in place and to examine whether there is evidence of tampering. Products or components should be inspected prior to use and periodically thereafter. Inspection requirements should also be included in contracts with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors and flow down to subcontractors, when relevant. Criticality analysis can help determine which systems and components are critical and should therefore be subjected to inspection. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis. The C-SCRM PMO can help identify critical systems and components, especially those that are used by multiple missions,	Functional	Intersects With	Technology Asset Inspections	AST-15.1	Mechanisms exist to physically and logically inspect critical technology assets to detect evidence of tampering.	5	Inspect the following systems or system components [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].