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 UPD1 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
Focal Document URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-161-r1-level-3.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description NIST SP 800-161 R1 Supplemental C-SCRM Guidance	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
AC-1	Policy and Procedures	Enterprises should specify and include in agreements (e.g., contracting language) access control policies for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers that have access control policies. These should include both physical and logical access to the supply chain and the information system. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtier contractors.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AC-1	Policy and Procedures	Enterprises should specify and include in agreements (e.g., contracting language) access control policies for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers that have access control policies. These should include both physical and logical access to the supply chain and the information system. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtier contractors.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities,
AC-1	Policy and Procedures	Enterprises should specify and include in agreements (e.g., contracting language) access control policies for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers that have access control policies. These should include both physical and logical access to the supply chain and the information system. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtier contractors.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AC-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-3(8)	Access Enforcement | Revocation of Access Authorizations	Prompt revocation is critical to ensure that suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers who no longer require access or who abuse or violate their access privilege are not able to access an enterprise's system. Enterprises should include in their agreements a requirement for contractors and sub-tier contractors to immediately return access credentials (e.g., tokens, PIV or CAC cards, etc.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrator enterprise to another with the same personnel supporting the contract. In that situation, the enterprise should disable the existing accounts, retire the old credentials, establish new accounts, and issue completely new	Functional	Equal	Revocation of Access Authorizations	IAC-20.6	Mechanisms exist to revoke logical and physical access authorizations.	10	Enforce the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [Assignment: organization-defined rules governing the timing of revocations of access authorizations].
AC-3(9)	Access Enforcement | Controlled Release	Information about the supply chain should be controlled for release between the enterprise and third parties. Information may be exchanged between the enterprise and its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The controlled release of enterprise information protects against risks associated with disclosure.	Functional	Equal	Controlled Release	DCH-03.3	Automated mechanisms exist to validate cybersecurity and data protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).	10	Release information outside of the system only if: (a) The receiving [Assignment: organization-defined system or system component] provides [Assignment: organization-defined controls]; and (b) [Assignment: organization-defined controls] are used to validate the appropriateness of the information designated for release.
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-4(6)	Information Flow Enforcement | Metadata	Enforce information flow control based on [Assignment: organization-defined metadata].	Functional	Equal	Metadata	NET-04.5	Mechanisms exist to enforce information flow controls based on metadata.	10	
AC-4(17)	Information Flow Enforcement | Domain Authentication	Within the C-SCRM context, enterprises should specify various source and destination points for information about the supply chain and information that flows through the supply chain. This is so that enterprises have visibility of information flow within the supply chain.	Functional	Equal	Cross Domain Authentication	NET-04.12	Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.	10	Uniquely identify and authenticate source and destination points by [Selection (one or more): organization; system; application; service; individual] for information transfer.
AC-4(19)	Information Flow Enforcement | Validation of Metadata	For C-SCRM, the validation of data and the relationship to its metadata are critical. Much of the data transmitted through the supply chain is validated with the verification of the associated metadata that is bound to it. Ensure that proper filtering and inspection is put in place for validation before allowing payloads into the supply chain	Functional	Equal	Metadata Validation	NET-04.13	Automated mechanisms exist to apply cybersecurity and/or data protection filters on metadata.	10	When transferring information between different security domains, implement [Assignment: organization-defined security or privacy policy filters] on metadata.
AC-4(21)	Information Flow Enforcement | Physical or Logical Separation of Information Flows	The enterprise should ensure the separation of the information system and supply chain information36 flow. Various mechanisms can be implemented, such as encryption methods (e.g., digital signing). Addressing information flow between the enterprise and its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers may be challenging, especially when leveraging public networks.	Functional	Equal	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	10	Separate information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].
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-6(6)	Least Privilege | Privileged Access by Non-organizational Users	Enterprises should ensure that protections are in place to prevent non-enterprise users from having privileged access to enterprise supply chain and related supply chain information. When enterprise users include independent consultants, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, relevant access requirements may need to use least privilege mechanisms to precisely define what information and/or components are accessible, for what duration, at what frequency, using what access methods, and by whom. Understanding what components are critical and non-critical can aid in understanding the level of detail that may need to be defined regarding least privilege access for non-enterprise users.	Functional	Equal	Privileged Access by Non-Organizational Users	IAC-05.2	Mechanisms exist to prohibit privileged access by non-organizational users.	10	Prohibit privileged access to the system by non-organizational users.
AC-17	Remote Access	For 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-17(6)	Remote Access | Protection of Mechanism Information	Enterprises should ensure that detailed requirements are properly defined and that access to information regarding the information system and supply chain is protected from unauthorized use and disclosure. Since supply chain data and metadata disclosure or access can have significant implications for an enterprise's mission processes, appropriate measures must be taken to vet both the supply chain and personnel processes to ensure that adequate protections are implemented. Ensure that remote access to such information is included in requirements.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	Protect information about remote access mechanisms from unauthorized use and disclosure.
AC-18	Wireless Access	An enterprise's supply chain may include wireless infrastructure that supports supply chain logistics (e.g., radio-frequency identification device [RFID] support, software call home features). Supply chain systems/components traverse the supply chain as they are moved from one location to another, whether within the enterprise's own environment or during delivery from system integrators or suppliers. Ensuring that appropriate and secure access mechanisms are in place within this supply chain enables the protection of the information systems and components, as well as logistics technologies and metadata used during shipping (e.g., within tracking sensors). The enterprise should explicitly define appropriate wireless access control mechanisms for the supply chain in policy and implement appropriate mechanisms.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and b. Authorize each type of wireless access to the system prior to allowing such connections.
AC-18	Wireless Access	An enterprise's supply chain may include wireless infrastructure that supports supply chain logistics (e.g., radio-frequency identification device [RFID] support, software call home features). Supply chain systems/components traverse the supply chain as they are moved from one location to another, whether within the enterprise's own environment or during delivery from system integrators or suppliers. Ensuring that appropriate and secure access mechanisms are in place within this supply chain enables the protection of the information systems and components, as well as logistics technologies and metadata used during shipping (e.g., within tracking sensors). The enterprise should explicitly define appropriate wireless access control mechanisms for the supply chain in policy and implement appropriate mechanisms.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and b. Authorize each type of wireless access to the system prior to allowing such connections.
AC-19	Access Control for Mobile Devices	The use of mobile devices (e.g., laptops, tablets, e-readers, smartphones, smartwatches) has become common in the supply chain. They are used in direct support of an enterprise's operations, as well as tracking, supply chain logistics, data as information systems, and components that traverse enterprise or systems integrator supply chains. Ensure that access control mechanisms are clearly defined and implemented where relevant when managing enterprise supply chain components. An example of such an implementation includes access control mechanisms implemented for use with remote handheld units in RFID for tracking components that traverse the supply chain. Access control mechanisms should also be implemented on any associated data and metadata tied to the devices.	Functional	Equal	Access Control For Mobile Devices	MDM-02	Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	10	a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and b. Authorize the connection of mobile devices to organizational systems.
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:

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-20(1)	Use of External Systems | Limits on Authorized Use	This enhancement helps limit exposure of the supply chain to the systems of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Equal	Limits of Authorized Use	DCH-13.1	Mechanisms exist to prohibit external parties, including Technology Assets, Applications and/or Services (TAAS), from storing, processing and transmitting data unless authorized individuals first: (1) Verifying the implementation of required security, compliance and/or resilience controls; or (2) Retaining a processing agreement with the entity hosting the external TAAS.	10	Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after: (a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or
AC-20(3)	Use of External Systems | Non-organizationally Owned Systems — Restricted Use	Devices that do not belong to the enterprise (e.g., bring your own device [BYOD] policies) increase the enterprise's exposure to cybersecurity risks throughout the supply chain. This includes devices used by suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Enterprises should review the use of non-enterprise devices by non-enterprise personnel and make a risk-based decision as to whether it will allow the use of such devices or furnish devices. Enterprises should furnish devices to those nonenterprise personnel who present unacceptable levels of risk.	Functional	Equal	Non-Organizationally Owned Technology Assets, Applications and/or Services (TAAS)	DCH-13.4	Mechanisms exist to restrict the use of non-organizationally owned Technology Assets, Applications and/or Services (TAAS) to process, store or transmit organizational information.	10	Restrict the use of non-organizationally owned systems or system components to process, store, or transmit organizational information using [Assignment: organization-defined restrictions].
AC-22	Publicly Accessible Content	Within the C-SCRM context, publicly accessible content may include Requests for Information, Requests for Proposal, or information about delivery of systems and components. This information should be reviewed to ensure that only appropriate content is released for public consumption, whether alone or with other information.	Functional	Equal	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	10	a. Designate individuals authorized to make information publicly accessible; b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included;
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.
AU-1	Policy and Procedures	audit and accountability policy and procedures to include auditing of the supply chain information systems and network. The audit and accountability policy and procedures should appropriately address tracking activities and their availability for other various supply chain activities, such as configuration management. Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers activities should not be included in such a policy unless those functions are performed within the acquirer's supply chain information systems and network. Audit and accountability policy procedures should appropriately address supplier audits as a way to examine the quality of a particular supplier and the risk they present to the enterprise and the enterprise's	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AU-1	Policy and Procedures	audit and accountability policy and procedures to include auditing of the supply chain information systems and network. The audit and accountability policy and procedures should appropriately address tracking activities and their availability for other various supply chain activities, such as configuration management. Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers activities should not be included in such a policy unless those functions are performed within the acquirer's supply chain information systems and network. Audit and accountability policy procedures should appropriately address supplier audits as a way to examine the quality of a particular supplier and the risk they present to the enterprise and the enterprise's	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AU-1	Policy and Procedures	audit and accountability policy and procedures to include auditing of the supply chain information systems and network. The audit and accountability policy and procedures should appropriately address tracking activities and their availability for other various supply chain activities, such as configuration management. Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers activities should not be included in such a policy unless those functions are performed within the acquirer's supply chain information systems and network. Audit and accountability policy procedures should appropriately address supplier audits as a way to examine the quality of a particular supplier and the risk they present to the enterprise and the enterprise's	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AU-2	Event Logging	software/hardware changes, failed attempts to access supply chain information systems, or the movement of source code. Information on such events should be captured by appropriate audit mechanisms and be traceable and verifiable. Information captured may include the type of event, date/time, length, and the frequency of occurrence. Among other things, auditing may help detect misuse of the supply chain information systems or network caused by insider threats. Logs are a key resource when identifying operational trends and long-term problems. As such, enterprises should incorporate reviewing logs at the contract renewal point for vendors to determine whether there is a systemic problem. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
AU-2	Event Logging	software/hardware changes, failed attempts to access supply chain information systems, or the movement of source code. Information on such events should be captured by appropriate audit mechanisms and be traceable and verifiable. Information captured may include the type of event, date/time, length, and the frequency of occurrence. Among other things, auditing may help detect misuse of the supply chain information systems or network caused by insider threats. Logs are a key resource when identifying operational trends and long-term problems. As such, enterprises should incorporate reviewing logs at the contract renewal point for vendors to determine whether there is a systemic problem. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
AU-3	Content of Audit Records	The audit records of a supply chain event should be securely handled and maintained in a manner that conforms to record retention requirements and preserves the integrity of the findings and the confidentiality of the record information and its sources as appropriate. In certain instances, such records may be used in administrative or legal proceedings. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Equal	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and	10	Ensure that audit records contain information that establishes the following: a. What type of event occurred; b. When the event occurred; c. Where the event occurred; d. Source of the event; e. Outcome of the event; and f. Identity of any individuals, subjects, or
AU-6	Audit Record Review, Analysis, and Reporting	The enterprise should ensure that both supply chain and information security auditable events are appropriately filtered and correlated for analysis and reporting. For example, if new maintenance or a patch upgrade is recognized to have an invalid digital signature, the identification of the patch arrival qualifies as a supply chain auditable event, while an invalid signature is an information security auditable event. The combination of these two events may provide information valuable to CSCRM. The enterprise should adjust the level of audit record review based on the risk changes (e.g., active threat intel, risk profile) on a specific vendor. Contracts should explicitly address how audit findings will be reported and adjudicated.	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. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity; b. Report findings to [Assignment: organization-defined personnel or roles]; and c. Adjust the level of audit record review, analysis,
AU-6	Audit Record Review, Analysis, and Reporting	The enterprise should ensure that both supply chain and information security auditable events are appropriately filtered and correlated for analysis and reporting. For example, if new maintenance or a patch upgrade is recognized to have an invalid digital signature, the identification of the patch arrival qualifies as a supply chain auditable event, while an invalid signature is an information security auditable event. The combination of these two events may provide information valuable to CSCRM. The enterprise should adjust the level of audit record review based on the risk changes (e.g., active threat intel, risk profile) on a specific vendor. Contracts should explicitly address how audit findings will be reported and adjudicated.	Functional	Intersects With	Audit Level Adjustments	MON-02.6	Mechanisms exist to adjust the level of audit review, analysis and reporting based on evolving threat information from law enforcement, industry associations or other credible sources of threat intelligence.	5	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity; b. Report findings to [Assignment: organization-defined personnel or roles]; and c. Adjust the level of audit record review, analysis,
AU-6(9)	Audit Record Review, Analysis, and Reporting | Correlation with Information from Nontechnical Sources	In a C-SCRM context, non-technical sources include changes to the enterprise's security or operational policy, changes to the procurement or contracting processes, and notifications from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers regarding plans to update, enhance, patch, or retire/dispose of a system/component.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.
AU-10	Non-repudiation	Enterprises should implement non-repudiation techniques to protect the originality and integrity of both information systems and the supply chain network. Examples of what may require non-repudiation include supply chain metadata that describes the components, supply chain communication, and delivery acceptance information. For information systems, examples may include patch or maintenance upgrades for software as well as component replacements in a large hardware system. Verifying that such components originate from the OEM is part of non-repudiation.	Functional	Equal	Non-Repudiation	MON-09	Mechanisms exist to utilize a non-repudiation capability to protect against an individual falsely denying having performed a particular action.	10	Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [Assignment: organization-defined actions to be covered by non-repudiation].
AU-10(2)	Non-repudiation | Validate Binding of Information Producer Identity	This enhancement validates the relationship of provenance and a component within the supply chain. Therefore, it ensures integrity of provenance.	Functional	Intersects With	Identity Binding	MON-09.1	Mechanisms exist to bind the identity of the information producer to the information generated.	5	(a) Validate the binding of the information producer identity to the information at [Assignment: organization-defined frequency]; and (b) Perform [Assignment: organization-defined actions] in the event of a validation error.
AU-10(3)	Non-repudiation | Chain of Custody	Chain of custody is fundamental to provenance and traceability in the supply chain. It also helps the verification of system and component integrity.	Functional	Intersects With	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5	Maintain reviewer or releaser credentials within the established chain of custody for information reviewed or released.
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	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,
AU-16	Cross-organizational Audit Logging	In a C-SCRM context, this control includes the enterprise's use of system integrator or external service provider infrastructure. Enterprises should add language to contracts on coordinating audit information requirements and information exchange agreements with vendors.	Functional	Intersects With	Cross-Organizational Monitoring	MON-14	Mechanisms exist to coordinate sanitized event logs among external organizations to identify anomalous events when event logs are shared across organizational boundaries, without giving away sensitive or critical business data.	5	Employ [Assignment: organization-defined methods] for coordinating [Assignment: organization-defined audit information] among external organizations when audit information is transmitted across organizational boundaries.
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-1	Policy and Procedures	Integrate the development and implementation of assessment and authorization policies and procedures for supply chain cybersecurity into the control assessment and authorization policy and related C-SCRM Strategy/Implementation Plan(s), policies, and system-level plans. To address cybersecurity risks throughout the supply chain, enterprises should develop a C-SCRM policy (or, if required, integrate into existing policies) to direct C-SCRM activities for control assessment and authorization. The C-SCRM policy should define C-SCRM roles and responsibilities within the enterprise for conducting control assessment and authorization, any dependencies among those roles, and the interaction among the roles. Enterprise-wide security and privacy risks should be assessed on an ongoing basis and include supply chain risk assessment results.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that: (a) Addresses purpose, scope, roles, responsibilities
CA-1	Policy and Procedures	Integrate the development and implementation of assessment and authorization policies and procedures for supply chain cybersecurity into the control assessment and authorization policy and related C-SCRM Strategy/Implementation Plan(s), policies, and system-level plans. To address cybersecurity risks throughout the supply chain, enterprises should develop a C-SCRM policy (or, if required, integrate into existing policies) to direct C-SCRM activities for control assessment and authorization. The C-SCRM policy should define C-SCRM roles and responsibilities within the enterprise for conducting control assessment and authorization, any dependencies among those roles, and the interaction among the roles. Enterprise-wide security and privacy risks should be assessed on an ongoing basis and include supply chain risk assessment results.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that: (a) Addresses purpose, scope, roles, responsibilities
CA-1	Policy and Procedures	Integrate the development and implementation of assessment and authorization policies and procedures for supply chain cybersecurity into the control assessment and authorization policy and related C-SCRM Strategy/Implementation Plan(s), policies, and system-level plans. To address cybersecurity risks throughout the supply chain, enterprises should develop a C-SCRM policy (or, if required, integrate into existing policies) to direct C-SCRM activities for control assessment and authorization. The C-SCRM policy should define C-SCRM roles and responsibilities within the enterprise for conducting control assessment and authorization, any dependencies among those roles, and the interaction among the roles. Enterprise-wide security and privacy risks should be assessed on an ongoing basis and include supply chain risk assessment results.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that: (a) Addresses purpose, scope, roles, responsibilities
CA-2	Control Assessments	Ensure that the control assessment plan incorporates relevant C-SCRM controls and control enhancements. The control assessment should cover the assessment of both information systems and the supply chain and ensure that an enterprise-relevant baseline set of controls and control enhancements are identified and used for the assessment. Control assessments can include information from supplier audits, reviews, and supply chain-related information. Enterprises should develop a strategy for collecting information, including a strategy for engaging with providers on supply chain risk assessments. Such collaboration helps enterprises leverage information from providers, reduce redundancy, identify potential courses of action for risk responses, and reduce the burden on providers. CSCRM personnel should review the control assessment.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and
CA-2	Control Assessments	Ensure that the control assessment plan incorporates relevant C-SCRM controls and control enhancements. The control assessment should cover the assessment of both information systems and the supply chain and ensure that an enterprise-relevant baseline set of controls and control enhancements are identified and used for the assessment. Control assessments can include information from supplier audits, reviews, and supply chain-related information. Enterprises should develop a strategy for collecting information, including a strategy for engaging with providers on supply chain risk assessments. Such collaboration helps enterprises leverage information from providers, reduce redundancy, identify potential courses of action for risk responses, and reduce the burden on providers. CSCRM personnel should review the control assessment.	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	5	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and

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
CA-2	Control Assessments	Ensure that the control assessment plan incorporates relevant C-SCRM controls and control enhancements. The control assessment should cover the assessment of both information systems and the supply chain and ensure that an enterprise-relevant baseline set of controls and control enhancements are identified and used for the assessment. Control assessments can include information from supplier audits, reviews, and supply chain-related information. Enterprises should develop a strategy for collecting information, including a strategy for engaging with providers on supply chain risk assessments. Such collaboration helps enterprises leverage information from providers, reduce redundancy, identify potential courses of action for risk responses, and reduce the burden on providers. CSCRM personnel should review the control assessment.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and
CA-2	Control Assessments	Ensure that the control assessment plan incorporates relevant C-SCRM controls and control enhancements. The control assessment should cover the assessment of both information systems and the supply chain and ensure that an enterprise-relevant baseline set of controls and control enhancements are identified and used for the assessment. Control assessments can include information from supplier audits, reviews, and supply chain-related information. Enterprises should develop a strategy for collecting information, including a strategy for engaging with providers on supply chain risk assessments. Such collaboration helps enterprises leverage information from providers, reduce redundancy, identify potential courses of action for risk responses, and reduce the burden on providers. CSCRM personnel should review the control assessment.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and
CA-2	Control Assessments	Ensure that the control assessment plan incorporates relevant C-SCRM controls and control enhancements. The control assessment should cover the assessment of both information systems and the supply chain and ensure that an enterprise-relevant baseline set of controls and control enhancements are identified and used for the assessment. Control assessments can include information from supplier audits, reviews, and supply chain-related information. Enterprises should develop a strategy for collecting information, including a strategy for engaging with providers on supply chain risk assessments. Such collaboration helps enterprises leverage information from providers, reduce redundancy, identify potential courses of action for risk responses, and reduce the burden on providers. CSCRM personnel should review the control assessment.	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and
CA-2(2)	Control Assessments | Specialized Assessments	Enterprises should use a variety of assessment techniques and methodologies, such as continuous monitoring, insider threat assessment, and malicious user assessment. These assessment mechanisms are context-specific and require the enterprise to understand its supply chain and to define the required set of measures for assessing and verifying that appropriate protections have been implemented.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management;	5	Include as part of control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced]; [Selection (one or more): in-depth monitoring; security instrumentation; automated security test cases; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; data leakage or data loss assessment;
CA-2(3)	Control Assessments | Leveraging Results from External Organizations	For C-SCRM, enterprises should use external security assessments for suppliers, developers, system integrators, external system service providers, and other ICT/OTrelated service providers. External assessments include certifications, third-party assessments, and – in the federal context – prior assessments performed by other departments and agencies. Certifications from the International Enterprise for Standardization (ISO), the National Information Assurance Partnership (Common Criteria), and the Open Group Trusted Technology Forum (OTTF) may also be used by non-federal and federal enterprises alike, if such certifications meet agency needs.	Functional	Equal	Third-Party Assessment Reciprocity	IAO-02.3	Mechanisms exist to accept and respond to the results of external assessments that are performed by impartial, external organizations.	10	Leverage the results of control assessments performed by [Assignment: organization-defined external organization] on [Assignment: organization-defined system] when the assessment meets [Assignment: organization-defined requirements].
CA-3	Information Exchange	with developers, system integrators, external system service providers, other ICT/OT-related service providers, and – in some cases – suppliers. Proper serviceslevel 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 environment 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; [Assignment: organization-defined type of
CA-5	Plan of Action and Milestones	exists for C-SCRM and includes both information systems and the supply chain. The C-SCRM POA&M should include tasks to be accomplished with a recommendation for completion before or after system authorization, the resources required to accomplish the tasks, milestones established to meet the tasks, and the scheduled completion dates for the milestones and tasks. The enterprise should include relevant weaknesses, the impact of weaknesses on information systems or the supply chain, any remediation to address weaknesses, and any continuous monitoring activities in its C-SCRM POA&M. The C-SCRM POA&M should be included as part of the authorization	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection;	5	a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and b. Update existing plan of action and milestones [Assignment: organization-defined frequency] based
CA-6	Authorization	Authorizing officials should include C-SCRM in authorization decisions. To accomplish this, supply chain risks and compensating controls documented in C-SCRM Plans or system security plans and the C-SCRM POA&M should be included in the authorization package as part of the decision-making process. Risks should be determined and associated compensating controls selected based on the output of criticality, threat, and vulnerability analyses. Authorizing officials may use the guidance in Section 2 of this document as well as NISTIR 8179 to guide the assessment process.	Functional	Equal	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	10	a. Assign a senior official as the authorizing official for the system; b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems; c. Ensure that the authorizing official for the system, before commencing operations: 1. Accepts the use of common controls inherited by
CA-7(3)	Continuous Monitoring | Trend Analyses	The information gathered during continuous monitoring/trend analyses serves as input into C-SCRM decisions, including criticality analysis, vulnerability and threat analysis, and risk assessments. It also provides information that can be used in incident response and potentially identify a supply chain cybersecurity compromise, including an insider threat.	Functional	Equal	Trend Analysis Reporting	MON-06.2	Mechanisms exist to employ trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.	10	Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.
CM-1	Policy and Procedures	to the enterprise's ability to establish the provenance of components, including tracking and tracing them through the SDLC and the supply chain. A properly defined and implemented configuration management capability provides greater assurance throughout the SDLC and the supply chain that components are authentic and have not been inappropriately modified. When defining a configuration management policy and procedures, enterprises should address the full SDLC, including procedures for introducing and removing components to and from the enterprise's information system boundary. A configuration management policy should incorporate configuration items, data retention for configuration items and corresponding metadata, and tracking of the configuration item and its metadata. The enterprise should coordinate with suppliers, developers, system integrators, external system	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
CM-1	Policy and Procedures	to the enterprise's ability to establish the provenance of components, including tracking and tracing them through the SDLC and the supply chain. A properly defined and implemented configuration management capability provides greater assurance throughout the SDLC and the supply chain that components are authentic and have not been inappropriately modified. When defining a configuration management policy and procedures, enterprises should address the full SDLC, including procedures for introducing and removing components to and from the enterprise's information system boundary. A configuration management policy should incorporate configuration items, data retention for configuration items and corresponding metadata, and tracking of the configuration item and its metadata. The enterprise should coordinate with suppliers, developers, system integrators, external system	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
CM-1	Policy and Procedures	to the enterprise's ability to establish the provenance of components, including tracking and tracing them through the SDLC and the supply chain. A properly defined and implemented configuration management capability provides greater assurance throughout the SDLC and the supply chain that components are authentic and have not been inappropriately modified. When defining a configuration management policy and procedures, enterprises should address the full SDLC, including procedures for introducing and removing components to and from the enterprise's information system boundary. A configuration management policy should incorporate configuration items, data retention for configuration items and corresponding metadata, and tracking of the configuration item and its metadata. The enterprise should coordinate with suppliers, developers, system integrators, external system	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
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-2(6)	Baseline Configuration | Development and Test Environments	The enterprise should maintain or require the maintenance of a baseline configuration of applicable suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers' development, test (and staging, if applicable) environments, and any configuration of interfaces.	Functional	Equal	Development & Test Environment Configurations	CFG-02.4	Mechanisms exist to manage baseline configurations for development and test environments separately from operational baseline configurations to minimize the risk of unintentional changes.	10	Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration.
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-3(1)	Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes	Enterprises should define a set of system changes that are critical to the protection of the information system and the underlying or interoperating systems and networks. These changes may be defined based on a criticality analysis (including components, processes, and functions) and where vulnerabilities exist that are not yet remediated (e.g., due to resource constraints). The change control process should also monitor for changes that may affect an existing security control to ensure that this control continues to function as required.	Functional	Equal	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	10	Use [Assignment: organization-defined automated mechanisms] to: (a) Document proposed changes to the system; (b) Notify [Assignment: organization-defined approval authorities] of proposed changes to the system and request change approval; (c) Highlight proposed changes to the system that have not been approved or disapproved within
CM-3(2)	Configuration Change Control | Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing implementation of the changes.	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	5	Test, validate, and document changes to the system before finalizing the implementation of the changes.
CM-3(2)	Configuration Change Control | Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing implementation of the changes.	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	5	Test, validate, and document changes to the system before finalizing the implementation of the changes.
CM-3(4)	Configuration Change Control | Security and Privacy Representatives	Require enterprise security and privacy representatives to be members of the configuration change control function.	Functional	Equal	Security, Compliance & Resilience Representative for Asset Lifecycle Changes	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data protection representative in the configuration change control review process.	10	Require [Assignment: organization-defined security and privacy representatives] to be members of the [Assignment: organization-defined configuration change control element].
CM-3(8)	Configuration Change Control | Prevent or Restrict Configuration Changes	Prevent or restrict changes to the configuration of the system under enterprise-defined circumstances.	Functional	Equal	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	10	Prevent or restrict changes to the configuration of the system under the following circumstances: [Assignment: organization-defined circumstances].
CM-4	Impact Analyses	Enterprises should take changes to the information system and underlying or interoperable systems and networks under consideration to determine whether the impact of these changes affects existing security controls and warrants additional or different protection to maintain an acceptable level of cybersecurity risk throughout the supply chain. Ensure that stakeholders, such as system engineers and system security engineers, are included in the impact analysis activities to provide their perspectives for C-SCRM. NIST SP 800-53, Rev. 5 control enhancement CM-4 (1) is a mechanism that can be used to protect the information system from vulnerabilities that may be introduced through the test environment.	Functional	Equal	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	10	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.
CM-4(1)	Impact Analyses | Separate Test Environments	Analyze changes to the system in a separate test environment before implementing them into an operational environment, and look for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.	Functional	Equal	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	10	Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.
CM-5	Access Restrictions for Change	Enterprises should ensure that requirements regarding physical and logical access restrictions for changes to the information systems and networks are defined and included in the enterprise's implementation of access restrictions. Examples include access restriction for changes to centrally managed processes for software component updates and the deployment of updates or patches.	Functional	Intersects With	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to Technology Assets, Applications and/or Services (TAAS).	5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.
CM-5	Access Restrictions for Change	Enterprises should ensure that requirements regarding physical and logical access restrictions for changes to the information systems and networks are defined and included in the enterprise's implementation of access restrictions. Examples include access restriction for changes to centrally managed processes for software component updates and the deployment of updates or patches.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.
CM-5(1)	Access Restrictions for Change | Automated Access Enforcement and Audit Records	Enterprises should implement mechanisms to ensure automated access enforcement and auditing of the information system and the underlying systems and networks.	Functional	Equal	Automated Access Enforcement / Auditing	CHG-04.1	Mechanisms exist to perform after-the-fact reviews of configuration change logs to discover any unauthorized changes.	10	(a) Enforce access restrictions using [Assignment: organization-defined automated mechanisms]; and (b) Automatically generate audit records of the enforcement actions.
CM-5(6)	Access Restrictions for Change | Limit Library Privileges	Enterprises should note that software libraries may be considered configuration items, access to which should be managed and controlled.	Functional	Equal	Library Privileges	CHG-04.5	Mechanisms exist to restrict software library privileges to those individuals with a pertinent business need for access.	10	Limit privileges to change software resident within software libraries.

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
CM-6	Configuration Settings	Enterprises should develop, document, and maintain secure baseline configurations for information systems and 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 Nation's Cybersecurity.	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; c. Identify, document, and approve any deviations
CM-6	Configuration Settings	Enterprises should develop, document, and maintain secure baseline configurations for information systems and 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 Nation's Cybersecurity.	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; c. Identify, document, and approve any deviations
CM-6(1)	Configuration Settings | Automated Management, Application, and Verification	The enterprise should, when feasible, employ automated mechanisms to manage, apply, and verify configuration settings.	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	Manage, apply, and verify configuration settings for [Assignment: organization-defined system components] using [Assignment: organization-defined automated mechanisms].
CM-6(2)	Configuration Settings | Respond to Unauthorized Changes	The enterprise should ensure that designated security or IT personnel are alerted to unauthorized changes to configuration settings. When suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers are responsible for such unauthorized changes, this qualifies as a C-SCRM incident that should be recorded and tracked to monitor trends. For a more comprehensive view, a specific, predefined set of C-SCRM stakeholders should assess the impact of unauthorized changes in the supply chain. When impact is assessed, relevant stakeholders should help define and implement appropriate mitigation strategies to ensure a comprehensive resolution.	Functional	Equal	Respond To Unauthorized Changes	CFG-02.8	Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents.	10	Take the following actions in response to unauthorized changes to [Assignment: organization-defined configuration settings]: [Assignment: organization-defined actions].
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-7(1)	Least Functionality | Periodic Review	Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Equal	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	10	(a) Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and (b) Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].
CM-7(4)	Least Functionality | Unauthorized Software — Deny-by-exception	Enterprises should define requirements and deploy appropriate processes to specify and detect software that is not allowed. This can be aided by defining a requirement to, at a minimum, not use disreputable or unauthorized software. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors	Functional	Equal	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	10	(a) Identify [Assignment: organization-defined software programs not authorized to execute on the system]; (b) Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; and (c) Review and update the list of unauthorized software programs [Assignment: organization-
CM-7(5)	Least Functionality | Authorized Software — Allow-by-exception	Enterprises should define requirements and deploy appropriate processes to specify allowable software. This can be aided by defining a requirement to use only reputable software. This can also include requirements for alerts when new software and updates to software are introduced into the enterprise's environment. An example of such requirements is to allow open source software only if the code is available for an enterprise's evaluation and determined to be acceptable for use	Functional	Equal	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	10	(a) Identify [Assignment: organization-defined software programs authorized to execute on the system]; (b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and (c) Review and update the list of authorized software programs [Assignment: organization-
CM-7(6)	Least Functionality | Confined Environments with Limited Privileges	The enterprise should ensure that code authentication mechanisms such as digital signatures are implemented when executing code to assure the integrity of software, firmware, and information on the information systems and networks.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	Require that the following user-installed software execute in a confined physical or virtual machine environment with limited privileges: [Assignment: organization-defined user-installed software].
CM-7(7)	Least Functionality | Code Execution in Protected Environments	The enterprise should obtain binary or machine-executable code directly from the OEM/developer or other acceptable, verified source.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	Allow execution of binary or machine-executable code only in confined physical or virtual machine environments and with the explicit approval of [Assignment: organization-defined personnel or roles] when such code is: (a) Obtained from sources with limited or no warranty; and/or (b) Without the provision of source code.
CM-7(8)	Least Functionality | Binary or Machine Executable Code	When exceptions are made to use software products without accompanying source code and with limited or no warranty because of compelling mission or operational requirements, approval by the authorizing official should be contingent upon the enterprise explicitly incorporating cybersecurity supply chain risk assessments as part of a broader assessment of such software products, as well as the implementation of compensating controls to address any identified and assessed risks.	Functional	Equal	Binary or Machine-Executable Code	END-06.7	Mechanisms exist to prohibit the use of binary or machine-executable code from sources with limited or no warranty and without access to source code.	10	(a) Prohibit the use of binary or machine-executable code from sources with limited or no warranty or without the provision of source code; and (b) Allow exceptions only for compelling mission or operational requirements and with the approval of the authorizing official.
CM-7(9)	Least Functionality | Prohibiting The Use of Unauthorized Hardware	Enterprises should define requirements and deploy appropriate processes to specify and detect hardware that is not allowed. This can be aided by defining a requirement to, at a minimum, not use disreputable or unauthorized hardware. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	(a) Identify [Assignment: organization-defined hardware components authorized for system use]; (b) Prohibit the use or connection of unauthorized hardware components; (c) Review and update the list of authorized hardware components [Assignment: organization-defined frequency].
CM-8	System Component Inventory	information includes, for example, hardware inventory specifications, software license information, software version 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	information includes, for example, hardware inventory specifications, software license information, software version 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-8(1)	System Component Inventory | Updates During Installation and Removal	When installing, updating, or removing an information system, information system component, or network component, the enterprise needs to update the inventory to ensure traceability for tracking critical components. In addition, the information system's configuration needs to be updated to ensure an accurate inventory of supply chain protections and then re-baselined accordingly.	Functional	Equal	Updates During Installations / Removals	AST-02.1	Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.	10	Update the inventory of system components as part of component installations, removals, and system updates.
CM-8(2)	System Component Inventory | Automated Maintenance	The enterprise should implement automated maintenance mechanisms to ensure that changes to component inventory for the information systems and networks are monitored for installation, update, and removal. When automated maintenance is performed with a predefined frequency and with the automated collation of relevant inventory information about each defined component, the enterprise should ensure that updates are available to relevant stakeholders for evaluation. Predefined frequencies for data collection should be less predictable in order to reduce the risk of an insider threat bypassing security mechanisms.	Functional	Equal	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	10	Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms].
CM-8(4)	System Component Inventory | Accountability Information	The enterprise should ensure that accountability information is collected for information system and network components. The system/component inventory information should identify those individuals who originate an acquisition as well as intended end users, including any associated personnel who may administer or use the system/components.	Functional	Equal	Accountability Information	AST-03.1	Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.	10	Include in the system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible and accountable for administering those components.
CM-8(6)	System Component Inventory | Assessed Configurations and Approved Deviations	Assessed configurations and approved deviations must be documented and tracked. Any changes to the baseline configurations of information systems and networks require a review by relevant stakeholders to ensure that the changes do not result in increased exposure to cybersecurity risks throughout the supply chain.	Functional	Equal	Approved Baseline Deviations	AST-02.4	Mechanisms exist to document and govern instances of approved deviations from established baseline configurations.	10	Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.
CM-8(7)	System Component Inventory | Centralized Repository	Enterprises may choose to implement centralized inventories that include components from all enterprise information systems, networks, and their components. Centralized repositories of inventories provide opportunities for efficiencies in accounting for information systems, networks, and their components. Such repositories may also help enterprises rapidly identify the location and responsible individuals of components that have been compromised, breached, or are otherwise in need of mitigation actions. The enterprise should ensure that centralized inventories include the supply chain-specific information required for proper component accountability (e.g., supply chain relevance and information system, network, or component owner).	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	Provide a centralized repository for the inventory of system components.
CM-8(8)	System Component Inventory | Automated Location Tracking	When employing automated mechanisms for tracking information system components by physical location, the enterprise should incorporate information system, network, and component tracking needs to ensure accurate inventory	Functional	Equal	Automated Location Tracking	AST-02.10	Mechanisms exist to track the geographic location of system components.	10	Support the tracking of system components by geographic location using [Assignment: organization-defined automated mechanisms].
CM-8(9)	System Component Inventory | Assignment of Components to Systems	When assigning components to systems, the enterprise should ensure that the information systems and networks with all relevant components are inventoried, marked, and properly assigned. This facilitates quick inventory of all components relevant to information systems and networks and enables tracking of components that are considered critical and require differentiating treatment as part of the information system and network protection activities.	Functional	Equal	Component Assignment	AST-02.11	Mechanisms exist to bind components to a specific system.	10	(a) Assign system components to a system; and (b) Receive an acknowledgement from [Assignment: organization-defined personnel or roles] of this assignment.
CM-8(10)	System Component Inventory | SBOMs for Open Source Projects	If an enterprise uses an open source project that does not have an SBOM and the enterprise requires one, the enterprise will need to 1) contribute SBOM generation to the open source project, 2) contribute resources to the project to add this capability, or 3) generate an SBOM on their first consumption of each version of the open source project that they use.	Functional	Intersects With	Open Source Software	CFG-04.1	Mechanisms exist to establish parameters for the secure use of open source software.	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
CM-8(10)	System Component Inventory | SBOMs for Open Source Projects	If an enterprise uses an open source project that does not have an SBOM and the enterprise requires one, the enterprise will need to 1) contribute SBOM generation to the open source project, 2) contribute resources to the project to add this capability, or 3) generate an SBOM on their first consumption of each version of the open source project that they use.	Functional	Intersects With	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
CM-8(10)	System Component Inventory | SBOMs for Open Source Projects	If an enterprise uses an open source project that does not have an SBOM and the enterprise requires one, the enterprise will need to 1) contribute SBOM generation to the open source project, 2) contribute resources to the project to add this capability, or 3) generate an SBOM on their first consumption of each version of the open source project that they use.	Functional	Intersects With	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security, compliance and resilience controls to be utilized within Technology Assets, Applications and/or Services (TAAS) in sufficient detail to permit analysis and testing of the controls.	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
CM-8(10)	System Component Inventory | SBOMs for Open Source Projects	If an enterprise uses an open source project that does not have an SBOM and the enterprise requires one, the enterprise will need to 1) contribute SBOM generation to the open source project, 2) contribute resources to the project to add this capability, or 3) generate an SBOM on their first consumption of each version of the open source project that they use.	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
CM-8(10)	System Component Inventory | SBOMs for Open Source Projects	If an enterprise uses an open source project that does not have an SBOM and the enterprise requires one, the enterprise will need to 1) contribute SBOM generation to the open source project, 2) contribute resources to the project to add this capability, or 3) generate an SBOM on their first consumption of each version of the open source project that they use.	Functional	Intersects With	Developer Architecture & Design	TDA-05	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that: (1) Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; (2) Accurately and completely describes the required security functionality and the allocation of security, compliance and resilience controls among physical	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
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

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
CM-9(1)	Configuration Management Plan | Assignment of Responsibility	Enterprises should ensure that all relevant roles are defined to address configuration management activities for information systems and networks. Enterprises should ensure that requirements and capabilities for configuration management are appropriately addressed or included in the following supply chain activities: requirements definition, development, testing, market research and analysis, procurement solicitations and contracts, component installation or removal, system integration, operations, and maintenance.	Functional	Equal	Assignment of Responsibility	CFG-01.1	Mechanisms exist to implement a segregation of duties for configuration management that prevents developers from performing production configuration management duties.	10	Assign responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.
CM-10	Software Usage Restrictions	Enterprises should ensure that licenses for software used within their information systems and networks are documented, tracked, and maintained. Tracking mechanisms should provide for the ability to trace users and the use of licenses to access control information and processes. As an example, when an employee is terminated, a "named user" license should be revoked, and the license documentation should be updated to reflect this change. 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	Software Usage Restrictions	CFG-04	Mechanisms exist to enforce software usage restrictions to comply with applicable contract agreements and copyright laws.	10	a. Use software and associated documentation in accordance with contract agreements and copyright laws; b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is
CM-10(1)	Software Usage Restrictions | Open-source Software	frameworks, reusable libraries' availability for testing and use, and any other information that may impact levels of exposure to cybersecurity risks throughout the supply chain. Numerous open source solutions are currently in use by enterprises, including in integrated development environments (IDEs) and web servers. The enterprise should: a. Track the use of OSS and associated documentation, b. Ensure that the use of OSS adheres to the licensing terms and that these terms are acceptable to the enterprise, c. Document and monitor the distribution of software as it relates to the licensing agreement to control copying and distribution, and d. Evaluate and periodically audit the OSS's supply chain as provided by the open source developer (e.g.,	Functional	Equal	Open Source Software	CFG-04.1	Mechanisms exist to establish parameters for the secure use of open source software.	10	Establish the following restrictions on the use of open-source software: [Assignment: organization-defined restrictions].
CM-11	User-installed Software	This control extends to the enterprise information system and network users who are not employed by the enterprise. These users may be suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Intersects With	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5	a. Establish [Assignment: organization-defined policies] governing the installation of software by users; b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; and c. Monitor policy compliance [Assignment: organization-defined frequency].
CM-11	User-installed Software	This control extends to the enterprise information system and network users who are not employed by the enterprise. These users may be suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Intersects With	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	a. Establish [Assignment: organization-defined policies] governing the installation of software by users; b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; and c. Monitor policy compliance [Assignment: organization-defined frequency].
CM-12	Information Location	Information that resides in different physical locations may be subject to different cybersecurity risks throughout the supply chain, depending on the specific location of the information. Components that originate or operate from different physical locations may also be subject to different supply chain risks, depending on the specific location of origination or operations. Enterprises should manage these risks through limiting access control and specifying allowable or disallowable geographic locations for backup/recovery, patching/upgrades, and information transfer/sharing. NIST SP 800-53, Rev. 5 control enhancement CM-12 (1) is a mechanism that can be used to enable automated location of components.	Functional	Equal	Information Location	DCH-24	Mechanisms exist to identify and document the location of information and the specific system components on which the information resides.	10	a. Identify and document the location of [Assignment: organization-defined information] and the specific system components on which the information is processed and stored; b. Identify and document the users who have access to the system and system components where the information is processed and stored; and c. Document changes to the location (i.e., system or
CM-12(1)	Information Location | Automated Tools to Support Information Location	Use automated tools to identify enterprise-defined information on enterprise-defined system components to ensure that controls are in place to protect enterprise information and individual privacy.	Functional	Equal	Automated Tools to Support Information Location	DCH-24.1	Automated mechanisms exist to identify by data classification type to ensure adequate security, compliance and resilience controls are in place to protect organizational information and individual data protection.	10	Use automated tools to identify [Assignment: organization-defined information by information type] on [Assignment: organization-defined system components] to ensure controls are in place to protect organizational information and individual privacy.
CM-13	Data Action Mapping	sensitive or classified information is necessary). Data action mapping should also be conducted to map Internet of Things (IoT) devices, embedded or stand-alone IoT systems, or IoT system of system data actions. Understanding what classified or IoT information is being processed, its sensitivity and/or effect on a physical thing or physical environment, how the sensitive or IoT information is being processed (e.g., if the data action is visible to an individual or is processed in another part of the system), and by whom provides a number of contextual factors that are important for assessing the degree of risk. Data maps can be illustrated in different ways, and the level of detail may vary based on the mission and business needs of the enterprise. The data map may be an overlay of any system design artifact that the enterprise is using. The development of this map may necessitate coordination	Functional	Equal	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive/regulated data is stored, transmitted or processed.	10	Develop and document a map of system data actions.
CM-14	Signed Components	Enterprises should verify that the acquired hardware and software components are genuine and valid by using digitally signed components from trusted certificate authorities. Verifying components before allowing installation helps enterprises reduce cybersecurity risks throughout the supply chain.	Functional	Intersects With	Signed Components	CHG-04.2	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.	5	Prevent the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.
CP-1	Policy and Procedures	Enterprises should integrate C-SCRM into the contingency planning policy and related SCRM Strategy/Implementation Plan, policies, and SCRM Plan. The policy should cover information systems and the supply chain network and, at a minimum, address scenarios such as: a. Unplanned component failure and subsequent replacement; b. Planned replacement related to feature improvements, maintenance, upgrades, and modernization; and c. Product and/or service disruption.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
CP-1	Policy and Procedures	Enterprises should integrate C-SCRM into the contingency planning policy and related SCRM Strategy/Implementation Plan, policies, and SCRM Plan. The policy should cover information systems and the supply chain network and, at a minimum, address scenarios such as: a. Unplanned component failure and subsequent replacement; b. Planned replacement related to feature improvements, maintenance, upgrades, and modernization; and c. Product and/or service disruption.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
CP-1	Policy and Procedures	Enterprises should integrate C-SCRM into the contingency planning policy and related SCRM Strategy/Implementation Plan, policies, and SCRM Plan. The policy should cover information systems and the supply chain network and, at a minimum, address scenarios such as: a. Unplanned component failure and subsequent replacement; b. Planned replacement related to feature improvements, maintenance, upgrades, and modernization; and c. Product and/or service disruption.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
CP-2	Contingency Plan	Enterprises should define and implement a contingency plan for the supply chain information systems and network to ensure that preparations are in place to mitigate the loss or degradation of data or operations. Contingencies should be put in place for the supply chain, network, information systems (especially critical components), and processes to ensure protection against compromise and provide appropriate failover and timely recovery to an acceptable state of operations.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	a. Develop a contingency plan for the system that: 1. Identifies essential mission and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential mission and
CP-2	Contingency Plan	Enterprises should define and implement a contingency plan for the supply chain information systems and network to ensure that preparations are in place to mitigate the loss or degradation of data or operations. Contingencies should be put in place for the supply chain, network, information systems (especially critical components), and processes to ensure protection against compromise and provide appropriate failover and timely recovery to an acceptable state of operations.	Functional	Intersects With	Ongoing Contingency Planning	BCD-06	Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes); (2) Processes (e.g., new, altered or decommissioned business practices, including third-party services) (3) Technologies (e.g., new, altered or decommissioned technologies); (4) Data (e.g., changes to data flows and/or data repositories); (5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or	5	a. Develop a contingency plan for the system that: 1. Identifies essential mission and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential mission and
CP-2(1)	Contingency Plan | Coordinate with Related Plans	Coordinate contingency plan development for supply chain risks with enterprise elements responsible for related plans.	Functional	Equal	Coordinate with Related Plans	BCD-01.1	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	10	Coordinate contingency plan development with organizational elements responsible for related plans.
CP-2(2)	Contingency Plan | Capacity Planning	This enhancement helps the availability of the supply chain network or information system components	Functional	Equal	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	10	Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.
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-2(8)	Contingency Plan | Identify Critical Assets	Ensure that critical assets (including hardware, software, and personnel) are identified and that appropriate contingency planning requirements are defined and applied to ensure the continuity of operations. A key step in this process is to complete a criticality analysis on components, functions, and processes to identify all critical assets. See Section 2 and NISTIR 8179 for additional guidance on criticality analyses.	Functional	Equal	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	10	Identify critical system assets supporting [Selection: all; essential] mission and business functions.
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
CP-3(1)	Contingency Training | Simulated Events	Enterprises should ensure that suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers who have roles and responsibilities in providing critical services are included in contingency training exercises.	Functional	Equal	Simulated Events	BCD-03.1	Mechanisms exist to incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.	10	Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.
CP-4	Contingency Plan Testing	Enterprises should ensure that critical suppliers are included in contingency testing. The enterprise – in coordination with the service provider(s) – should test continuity/resiliency capabilities, such as failover from a primary production site to a back-up site. This testing may occur separately from a training exercise or be performed during the exercise. Enterprises should reference their C-SCRM threat assessment output to develop scenarios to test how well the enterprise is able to withstand and/or recover from a C-SCRM threat event.	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests]. b. Review the contingency plan test results; and c. Initiate corrective actions, if needed.
CP-4	Contingency Plan Testing	Enterprises should ensure that critical suppliers are included in contingency testing. The enterprise – in coordination with the service provider(s) – should test continuity/resiliency capabilities, such as failover from a primary production site to a back-up site. This testing may occur separately from a training exercise or be performed during the exercise. Enterprises should reference their C-SCRM threat assessment output to develop scenarios to test how well the enterprise is able to withstand and/or recover from a C-SCRM threat event.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests]. b. Review the contingency plan test results; and c. Initiate corrective actions, if needed.
CP-6	Alternate Storage Site	When managed by suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, alternative storage sites are considered within an enterprise's supply chain network. Enterprises should apply appropriate cybersecurity supply chain controls to those storage sites.	Functional	Equal	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.	10	a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.
CP-6(1)	Alternate Storage Site | Separation from Primary Site	This enhancement helps the resiliency of the supply chain network, information systems, and information system components.	Functional	Equal	Separation from Primary Storage Site	BCD-08.1	Mechanisms exist to separate the alternate storage site from the primary storage site to reduce susceptibility to similar threats.	10	Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.
CP-7	Alternate Processing Site	When managed by suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, alternative storage sites are considered within an enterprise's supply chain. Enterprises should apply appropriate supply chain cybersecurity controls to those processing sites.	Functional	Equal	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	10	a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable;
CP-8	Telecommunications Services	Enterprises should incorporate alternative telecommunication service providers for their supply chain to support critical information systems.	Functional	Intersects With	Telecommunications Services Availability	BCD-10	Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.	5	Establish alternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or
CP-8(3)	Telecommunications Services | Separation of Primary and Alternate Providers	The separation of primary and alternative providers supports cybersecurity resilience of the supply chain.	Functional	Equal	Separation of Primary / Alternate Providers	BCD-10.2	Mechanisms exist to obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.	10	Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.
CP-8(4)	Telecommunications Services | Provider Contingency Plan	For C-SCRM, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, contingency plans should provide separation in infrastructure, service, process, and personnel, where appropriate.	Functional	Equal	Provider Contingency Plan	BCD-10.3	Mechanisms exist to contractually-require external service providers to have contingency plans that meet organizational contingency requirements.	10	(a) Require primary and alternate telecommunications service providers to have contingency plans; (b) Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and (c) Obtain evidence of contingency testing and training by providers [Assignment: organization-

FDE #	FDE Name	Focal Document Element (FDE) Description NIST SP 800-161 R1 Supplemental C-SCRM Guidance	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
CP-11	Alternate Communications Protocols	Enterprises should ensure that critical suppliers are included in contingency plans, training, and testing as part of incorporating alternative communications protocol capabilities to establish supply chain resilience.	Functional	Intersects With	Telecommunications Services Availability	BCD-10	Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.	5	Provide the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of operations.
IA-1	Policy and Procedures	The enterprise should – at enterprise-defined intervals – review, enhance, and update their identity and access management policies and procedures to ensure that critical roles and processes within the supply chain network are defined and that the enterprise's critical systems, components, and processes are identified for traceability. This should include the identity of critical components that may not have been considered under identification and authentication in the past. Note that providing identification for all items within the supply chain would be cost-prohibitive, and discretion should be used. The enterprise should update related C-SCRM Strategy/Implementation Plan(s), Policies, and C-SCRM Plans.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IA-1	Policy and Procedures	The enterprise should – at enterprise-defined intervals – review, enhance, and update their identity and access management policies and procedures to ensure that critical roles and processes within the supply chain network are defined and that the enterprise's critical systems, components, and processes are identified for traceability. This should include the identity of critical components that may not have been considered under identification and authentication in the past. Note that providing identification for all items within the supply chain would be cost-prohibitive, and discretion should be used. The enterprise should update related C-SCRM Strategy/Implementation Plan(s), Policies, and C-SCRM Plans.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IA-1	Policy and Procedures	The enterprise should – at enterprise-defined intervals – review, enhance, and update their identity and access management policies and procedures to ensure that critical roles and processes within the supply chain network are defined and that the enterprise's critical systems, components, and processes are identified for traceability. This should include the identity of critical components that may not have been considered under identification and authentication in the past. Note that providing identification for all items within the supply chain would be cost-prohibitive, and discretion should be used. The enterprise should update related C-SCRM Strategy/Implementation Plan(s), Policies, and C-SCRM Plans.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IA-2	Identification and Authentication (organizational Users)	Enterprises should ensure that identification and requirements are defined and applied for enterprise users accessing an ICT/OT system or supply chain network. An enterprise user may include employees, individuals deemed to have the equivalent status of employees (e.g., contractors, guest researchers, etc.), and system integrators fulfilling contractor roles. Criteria such as "duration in role" can aid in defining which identification and authentication mechanisms are used. The enterprise may choose to define a set of roles and associate a level of authorization to ensure proper implementation. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Equal	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	10	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.
IA-3	Device Identification and Authentication	Enterprises should implement capabilities to distinctly and positively identify devices and software within their supply chain and, once identified, verify that the identity is authentic. Devices that require unique device-to-device identification and authentication should be defined by type, device, or a combination of type and device. Software that requires authentication should be identified through a software identification tag (SWID) that enables verification of the software package and authentication of the enterprise releasing the software package.	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5	Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.
IA-4	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-4(6)	Identifier Management | Cross-organization Management	This enhancement helps the traceability and provenance of elements within the supply chain through the coordination of identifier management among the enterprise and its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. This includes information systems and components as well as individuals engaged in supply chain activities.	Functional	Equal	Cross-Organization Management	IAC-09.4	Mechanisms exist to coordinate username identifiers with external organizations for cross-organization management of identifiers.	10	Coordinate with the following external organizations for cross-organization management of identifiers: [Assignment: organization-defined external organizations].
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-5(5)	Authenticator Management | Change Authenticators Prior to Delivery	This enhancement verifies the chain of custody within the enterprise's supply chain.	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	Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.
IA-5(9)	Authenticator Management | Federated Credential Management	This enhancement facilitates provenance and chain of custody within the enterprise's supply chain.	Functional	Equal	Federated Credential Management	IAC-13.2	Mechanisms exist to federate credentials to allow cross-organization authentication of individuals and devices.	10	Use the following external organizations to federate credentials: [Assignment: organization-defined external organizations].
IA-8	Identification and Authentication (non-organizational Users)	Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers have the potential to engage the enterprise's supply chain for service delivery (e.g., development/integration services, product support, etc.). Enterprises should manage the establishment, auditing, use, and revocation of identification credentials and the authentication of non-enterprise users within the supply chain. Enterprises should also ensure promptness in performing identification and authentication activities, especially in the case of revocation management, to help mitigate exposure to cybersecurity risks throughout the supply chain such as those that arise due to insider threats.	Functional	Equal	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	10	Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.
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-3	Incident Response Testing	Enterprises should ensure that critical suppliers are included in and/or provided with incident response testing.	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests].
IR-4(6)	Incident Handling | Insider Threats	This enhancement helps limit exposure of the C-SCRM information systems, networks, and processes to insider threats. Enterprises should ensure that insider threat incident handling capabilities account for the potential of insider threats associated with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers' personnel with access to ICT/OT systems within the authorization boundary.	Functional	Intersects With	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5	Implement an incident handling capability for incidents involving insider threats.
IR-4(7)	Incident Handling | Insider Threats — Intra-organization Coordination	This enhancement helps limit the exposure of C-SCRM information systems, networks, and processes to insider threats. Enterprises should ensure that insider threat coordination includes suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Intersects With	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5	Coordinate an incident handling capability for insider threats that includes the following organizational entities [Assignment: organization-defined entities].
IR-4(11)	Incident Handling | Integrated Incident Response Team	An enterprise should include a forensics team and/or capability as part of an integrated incident response team for supply chain incidents. Where relevant and practical, integrated incident response teams should also include necessary geographical representation as well as suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Equal	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	10	Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in [Assignment: organization-defined time period].
IR-5	Incident Monitoring	Enterprises should ensure that agreements with suppliers include requirements to track and document incidents, response decisions, and activities.	Functional	Equal	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	10	Track and document incidents.
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.

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-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-2(2)	Controlled Maintenance | Automated Maintenance Activities	Enterprises should ensure that all automated maintenance activities for supply chain systems and networks are controlled and managed according to the maintenance policy. Examples of automated maintenance activities can include COTS product patch updates, call home features with failure notification feedback, etc. Managing these activities may require establishing staging processes with appropriate supporting mechanisms to provide vetting or filtering as appropriate. Staging processes may be especially important for critical systems and components.	Functional	Equal	Automated Maintenance Activities	MNT-02.1	Automated mechanisms exist to schedule, conduct and document maintenance and repairs.	10	(a) Schedule, conduct, and document maintenance, repair, and replacement actions for the system using [Assignment: organization-defined automated mechanisms]; and (b) Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.
MA-3	Maintenance Tools	Maintenance tools are considered part of the supply chain. They also have a supply chain of their own. C-SCRM should be integrated when the enterprise acquires or upgrades a maintenance tool (e.g., an update to the development environment or testing tool), including during the selection, ordering, storage, and integration of the maintenance tool. The enterprise should perform continuous review and approval of maintenance tools, including those maintenance tools in use by external service providers. The enterprise should also integrate C-SCRM when evaluating replacement parts for maintenance tools. This control may be performed at both Level 2 and Level 3, depending on how an agency handles the acquisition, operations, and oversight of maintenance tools.	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5	a. Approve, control, and monitor the use of system maintenance tools; and b. Review previously approved system maintenance tools [Assignment: organization-defined frequency].
MA-3(1)	Maintenance Tools | Inspect Tools	The enterprise should deploy acceptance testing to verify that the maintenance tools of the ICT supply chain infrastructure are as expected. Maintenance tools should be authorized with appropriate paperwork, verified as claimed through initial verification, and tested for vulnerabilities, appropriate security configurations, and stated functionality.	Functional	Equal	Inspect Tools	MNT-04.1	Mechanisms exist to inspect maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.	10	Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.
MA-3(2)	Maintenance Tools | Inspect Media	The enterprise should verify that the media containing diagnostic and test programs that suppliers use on the enterprise's information systems operates as expected and provides only required functions. The use of media from maintenance tools should be consistent with the enterprise's policies and procedures and pre-approved. Enterprises should also ensure that the functionality does not exceed that which was agreed upon.	Functional	Equal	Inspect Media	MNT-04.2	Mechanisms exist to check media containing diagnostic and test programs for malicious code before the media are used.	10	Check media containing diagnostic and test programs for malicious code before the media are used in the system.
MA-3(3)	Maintenance Tools | Prevent Unauthorized Removal	chain risks, such as unauthorized modification, replacement with counterfeit, or malware insertion while the tool is outside of the enterprise's control. Systems and network maintenance tools can include an integrated development environment (IDE), testing, or vulnerability scanning. For C-SCRM, it is important that enterprises should explicitly authorize, track, and audit any removal of maintenance tools. Once systems and network tools are allowed access to an enterprise/information system, they should remain the property/asset of the system owner and tracked if removed and used elsewhere in the enterprise. ICT maintenance tools either currently in use or in storage should not be allowed to leave the enterprise's premises until they are properly vetted for removal (i.e., maintenance tool removal should not exceed in scope what was authorized for removal and should be completed in accordance with	Functional	Equal	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.	10	Prevent the removal of maintenance equipment containing organizational information by: (a) Verifying that there is no organizational information contained on the equipment; (b) Sanitizing or destroying the equipment; (c) Retaining the equipment within the facility; or (d) Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly
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-4(3)	Nonlocal Maintenance | Comparable Security and Sanitization	enterprise should require that suppliers, developers, system integrators, external system service providers, or other ICT/OT-related service providers perform any nonlocal maintenance or diagnostic services on systems or system components, the enterprise should ensure that: • Appropriate measures are taken to verify that the nonlocal environment meets appropriate security levels for maintenance and diagnostics per agreements between the enterprise and vendor; • Appropriate levels of sanitizing are completed to remove any enterprise-specific data residing in components; and • Appropriate diagnostics are completed to ensure that components are sanitized, preventing malicious insertion prior to returning to the enterprise system or supply chain network. The enterprise should require its prime	Functional	Equal	Remote Maintenance Comparable Security & Sanitization	MNT-05.6	Mechanisms exist to require Technology Assets, Applications and/or Services (TAAS) performing remote, non-local maintenance and/or diagnostic services implement a security capability comparable to the capability implemented on the system being serviced.	10	(a) Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or (b) Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational
MA-5	Maintenance Personnel	Maintenance personnel may be employed by suppliers, developers, system integrators, external system service providers, or other ICT/OT-related service providers. As such, appropriate protections should be in place to manage associated risks. The same controls applied to internal maintenance personnel should be applied to any contractor personnel who performs a similar maintenance role and enforced through contractual agreements with their external service providers.	Functional	Equal	Authorized Maintenance Personnel	MNT-06	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	10	a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel; b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and c. Designate organizational personnel with required access authorizations and technical competence to
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
MA-6	Timely Maintenance	manufacturer (OEM), authorized distributor, or authorized resellers and ensure appropriate lead times if OEMs are not available, it is preferred to acquire from authorized distributors. If an OEM or an authorized distributor is not available, then it is preferred to acquire from an authorized reseller. Enterprises should obtain verification on whether the distributor or reseller is authorized. Where possible, enterprises should use an authorized distributor/dealer approved list. If the only alternative is to purchase from a non-authorized distributor or secondary market, a risk assessment should be performed, including revisiting the criticality and threat analysis to identify additional risk mitigations to be used. For example, the enterprise should check the supply source for a history of counterfeits, inappropriate practices, or a criminal record. See Section 2 for criticality and threat analysis details. The	Functional	Equal	Timely Maintenance	MNT-03	Mechanisms exist to obtain maintenance support and/or spare parts for Technology Assets, Applications and/or Services (TAAS) within a defined Recovery Time Objective (RTO).	10	Obtain maintenance support and/or spare parts for [Assignment: organization-defined system components] within [Assignment: organization-defined time period] of failure.
MA-7	Field Maintenance	Enterprises should use trusted facilities when additional rigor and quality control checks are needed, if at all practical or possible. Trusted facilities should be on an approved list and have additional controls in place.	Functional	Equal	Field Maintenance	MNT-08	Mechanisms exist to securely conduct field maintenance on geographically deployed assets.	10	Restrict or prohibit field maintenance on [Assignment: organization-defined systems or system components] to [Assignment: organization-defined trusted maintenance facilities].
MA-8	Maintenance Monitoring and Information Sharing	Tracking the failure rates of components provides valuable information to the acquirer to help plan for contingencies, alternative sources of supply, and replacements. Failure rates are also useful for monitoring the quality and reliability of systems and components. This information provides useful feedback to suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers for corrective action and continuous improvement. In Level 2, agencies should track and communicate the failure rates to suppliers (OEM and/or an authorized distributor). The failure rates and the issues that can indicate failures, including root causes, should be identified by an enterprise's technical personnel (e.g., developers, administrators, or maintenance engineers) in Level 3 and communicated to	Functional	Equal	Maintenance Monitoring	MNT-11	Mechanisms exist to maintain situational awareness of the quality and reliability of systems and components through tracking maintenance activities and component failure rates.	10	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
MA-8	Maintenance Monitoring and Information Sharing	Tracking the failure rates of components provides valuable information to the acquirer to help plan for contingencies, alternative sources of supply, and replacements. Failure rates are also useful for monitoring the quality and reliability of systems and components. This information provides useful feedback to suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers for corrective action and continuous improvement. In Level 2, agencies should track and communicate the failure rates to suppliers (OEM and/or an authorized distributor). The failure rates and the issues that can indicate failures, including root causes, should be identified by an enterprise's technical personnel (e.g., developers, administrators, or maintenance engineers) in Level 3 and communicated to Level 2. These individuals are able to verify the problem and identify	Functional	Intersects With	Predictable Failure Analysis	SEA-07	Mechanisms exist to determine the Mean Time to Failure (MTTF) for system components in specific environments of operation.	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
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-1	Policy and Procedures	The enterprise should integrate C-SCRM practices and requirements into their own physical and environmental protection policy and procedures. The degree of protection should be commensurate with the degree of integration. The physical and environmental protection policy should ensure that the physical interfaces of the supply chain have adequate protection and audit for such protection.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
PE-1	Policy and Procedures	The enterprise should integrate C-SCRM practices and requirements into their own physical and environmental protection policy and procedures. The degree of protection should be commensurate with the degree of integration. The physical and environmental protection policy should ensure that the physical interfaces of the supply chain have adequate protection and audit for such protection.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among

FDE #	FDE Name	Focal Document Element (FDE) Description NIST SP 800-161 R1 Supplemental C-SCRM Guidance	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
PE-1	Policy and Procedures	The enterprise should integrate C-SCRM practices and requirements into their own physical and environmental protection policy and procedures. The degree of protection should be commensurate with the degree of integration. The physical and environmental protection policy should ensure that the physical interfaces of the supply chain have adequate protection and audit for such protection.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
PE-2	Physical Access Authorizations	Enterprises should ensure that only authorized individuals with a need for physical access have access to 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, individual is permitted physical access during normal business hours, etc.).	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-2(1)	Physical Access Authorizations | Access by Position or Role	Role-based authorizations for physical access should include federal (e.g., agency/department employees) and non-federal employees (e.g., suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers). When role-based authorization is used, the type and level of access allowed for that role or position must be pre-established and documented.	Functional	Equal	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	10	Authorize physical access to the facility where the system resides based on position or role.
PE-3	Physical Access Control	Physical access control should include individuals and enterprises engaged in the enterprise's supply chain. A vetting process based on enterprise-defined requirements and policy should be in place prior to granting access to the supply chain infrastructure and any relevant elements. Access establishment, maintenance, and revocation processes should meet enterprise access control policy rigor. The speed of revocation for suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers who need access to physical facilities and data centers – either enterprise-owned or external service provider-owned – should be managed in accordance with the activities performed in their contracts. Prompt revocation is critical when either individual or enterprise need no longer exists.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	a. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by: 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress and egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems or devices];
PE-3(1)	Physical Access Control | System Access	Physical access controls should be extended to contractor personnel. Any contractor resources that provid services support with physical access to the supply chain infrastructure and any relevant elements should adhere to access controls. Policies and procedures should be consistent with those applied to employee personnel with similar levels of physical access.	Functional	Equal	Access To Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility.	10	Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].
PE-3(2)	Physical Access Control | Facility and Systems	When determining the extent, frequency, and/or randomness of security checks of facilities, enterprises should account for exfiltration risks that result from covert listening devices. Such devices may include wiretaps, roving bugs, cell site simulators, and other eavesdropping technologies that can transfer sensitive information out of the enterprise.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	Perform security checks [Assignment: organization-defined frequency] at the physical perimeter of the facility or system for exfiltration of information or removal of system components.
PE-3(5)	Physical Access Control | Logical Tampering Protection	Tamper protection is critical for reducing cybersecurity risk in products. The enterprise should implement validated tamper protection techniques within the supply chain. For critical products, the enterprise should require and assess whether and to what extent a supplier has implemented tamper protection mechanisms. The assessment may also include whether and how such mechanisms are required and applied by the supplier's upstream supply chain entities.	Functional	Equal	Mobile Device Tampering	MDM-04	Mechanisms exist to protect mobile devices from tampering through inspecting devices returning from locations that the organization deems to be of significant risk, prior to the device being connected to the organization's network.	10	Employ [Assignment: organization-defined anti-tamper technologies] to [Selection (one or more): detect; prevent] physical tampering or alteration of [Assignment: organization-defined hardware components] within the system.
PE-6	Monitoring Physical Access	Individuals who physically access the enterprise or external service provider's facilities, data centers, information, or physical asset(s) – including via the supply chain – may be employed by the enterprise's employees, on-site or remotely located contractors, visitors, other third parties (e.g., maintenance personnel under contract with the contractor enterprise), or an individual affiliated with an enterprise in the upstream supply chain. The enterprise should monitor these individuals' activities to reduce cybersecurity risks throughout the supply chain or require monitoring in agreements.	Functional	Equal	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	10	a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents; b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and c. Coordinate results of reviews and investigations
PE-16	Delivery and Removal	This control enhancement reduces cybersecurity risks that arise during the physical delivery and removal of hardware components from the enterprise's information systems or supply chain. This includes transportation security, the validation of delivered components, and the verification of sanitization procedures. Risk-based considerations include component mission criticality as well as the development, operational, or maintenance environment (e.g., classified integration and test laboratory).	Functional	Equal	Delivery & Removal	PES-10	Physical security mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access.	10	a. Authorize and control [Assignment: organization-defined types of system components] entering and exiting the facility; and b. Maintain records of the system components.
PE-17	Alternate Work Site	The enterprise should incorporate protections to guard against cybersecurity risks associated with enterprise employees or contractor personnel within or accessing the supply chain infrastructure using alternative work sites. This can include third-party personnel who may also work from alternative worksites.	Functional	Equal	Alternate Work Site	PES-11	Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	10	a. Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees; b. Employ the following controls at alternate work sites: [Assignment: organization-defined controls]; c. Assess the effectiveness of controls at alternate work sites; and d. Provide a means for employees to communicate
PE-18	Location of System Components	Physical and environmental hazards or disruptions have an impact on the availability of products that are or will be acquired and physically transported to the enterprise's locations. For example, enterprises should incorporate the manufacturing, warehousing, or the distribution location of information system components that are critical for agency operations when planning for alternative suppliers for these components.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	Position system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.
PE-20	Asset Monitoring and Tracking	The enterprise should, whenever possible and practical, use asset location technologies to track systems and components transported between entities across the supply chain, between protected areas, or in storage awaiting implementation, testing, maintenance, or disposal. Methods include RFID, digital signatures, or blockchains. These technologies help protect against: a. Diverting the system or component for counterfeit replacement; b. The loss of confidentiality, integrity, or availability of the system or component function and data (including data contained within the component and data about the component); and c. Interrupting supply chain and logistics processes for critical components. In addition to providing protection	Functional	Equal	Asset Monitoring and Tracking	PES-14	Physical security mechanisms exist to employ asset location technologies that track and monitor the location and movement of organization-defined assets within organization-defined controlled areas.	10	Employ [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas].
PE-23	Facility Location	Enterprises should incorporate the facility location (e.g., data centers) when assessing risks associated with 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	Enterprises should incorporate the facility location (e.g., data centers) when assessing risks associated with 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	Enterprises should incorporate the facility location (e.g., data centers) when assessing risks associated with 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	Enterprises should incorporate the facility location (e.g., data centers) when assessing risks associated with 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	Enterprises should incorporate the facility location (e.g., data centers) when assessing risks associated with 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	Enterprises should incorporate the facility location (e.g., data centers) when assessing risks associated with 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;
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;
PL-4	Rules of Behavior	The rules of behavior apply to contractor personnel and internal agency personnel. Contractor enterprises are responsible for ensuring that their employees follow applicable rules of behavior. Individual contractors should not be granted access to agency systems or data until they have acknowledged and demonstrated compliance with this control. Failure to meet this control can result in the removal of access for such individuals.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy; b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of
PL-4	Rules of Behavior	The rules of behavior apply to contractor personnel and internal agency personnel. Contractor enterprises are responsible for ensuring that their employees follow applicable rules of behavior. Individual contractors should not be granted access to agency systems or data until they have acknowledged and demonstrated compliance with this control. Failure to meet this control can result in the removal of access for such individuals.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy; b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of
PL-4	Rules of Behavior	The rules of behavior apply to contractor personnel and internal agency personnel. Contractor enterprises are responsible for ensuring that their employees follow applicable rules of behavior. Individual contractors should not be granted access to agency systems or data until they have acknowledged and demonstrated compliance with this control. Failure to meet this control can result in the removal of access for such individuals.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy; b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of
PL-7	Concept of Operations	The concept of operations (CONOPS) should describe how the enterprise intends to operate the system from the perspective of C-SCRM. It should integrate C-SCRM and be managed and updated throughout the applicable system's SDLC to address cybersecurity risks throughout the supply chain.	Functional	Equal	Security Concept Of Operations (CONOPS)	OPS-02	Mechanisms exist to develop a security Concept of Operations (CONOPS), or a similarly-defined plan for achieving cybersecurity objectives, that documents management, operational and technical measures implemented to apply defense-in-depth techniques that is communicated to all appropriate stakeholders.	10	a. Develop a Concept of Operations (CONOPS) for the system describing how the organization intends to operate the system from the perspective of information security and privacy; and b. Review and update the CONOPS [Assignment: organization-defined frequency].
PL-8	Security and Privacy Architectures	Security and privacy architecture defines and directs the implementation of security and privacy-protection methods, mechanisms, and capabilities to the underlying systems and networks, as well as the information system that is being created. Security architecture is fundamental to CSCRM because it helps to ensure that security is built-in throughout the SDLC. Enterprises should consider implementing zero-trust architectures and should ensure that the security architecture is well understood by system developers/engineers and system security engineers. This control applies to both federal agency and non-federal agency employees.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5	a. Develop security and privacy architectures for the system that: 1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information; 2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
PL-8(2)	Security and Privacy Architectures | Supplier Diversity	providers, and other ICT/OT-related service providers. The enterprise should plan for the potential replacement of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers in case one is no longer able to meet the enterprise's requirements (e.g., company goes out of business or does not meet contractual obligations). Where applicable, contracts should be worded so that different parts can be replaced with a similar model with similar prices from a different manufacturer if certain events occur (e.g., obsolescence, poor performance, production issues, etc.). Incorporate supplier diversity for off-the-shelf (commercial or government) components during acquisition security assessments. The evaluation of alternatives should include, for example, feature parity, interoperability, commodity	Functional	Intersects With	Supplier Diversity	TDA-03.1	Mechanisms exist to obtain security, compliance and resilience technologies from different suppliers to minimize supply chain risk.	5	Require that [Assignment: organization-defined controls] allocated to [Assignment: organization-defined locations and architectural layers] are obtained from different suppliers.
PL-10	Baseline Selection	Enterprises should include C-SCRM controls in their control baselines. Enterprises should identify and select C-SCRM controls based on the C-SCRM requirements identified within each of the levels. A C-SCRM PMO may assist in identifying C-SCRM control baselines that meet common C-SCRM requirements for different groups, communities of interest, or the enterprise as a whole	Functional	Equal	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.	10	Select a control baseline for the system.

FDE #	FDE Name	Focal Document Element (FDE) Description NIST SP 800-161 R1 Supplemental C-SCRM Guidance	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
PM-4	Plan of Action and Milestones Process	C-SCRM items should be included in the POA&M at all levels. Organizations should develop POA&Ms based on C-SCRM assessment reports. POA&M should be used by organizations to describe planned actions to correct the deficiencies in C-SCRM controls identified during assessment and the continuous monitoring of progress against those actions.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems: 1. Are developed and maintained; 2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational
PM-4	Plan of Action and Milestones Process	C-SCRM items should be included in the POA&M at all levels. Organizations should develop POA&Ms based on C-SCRM assessment reports. POA&M should be used by organizations to describe planned actions to correct the deficiencies in C-SCRM controls identified during assessment and the continuous monitoring of progress against those actions.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection;	5	a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems: 1. Are developed and maintained; 2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational
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-11	Mission and Business Process Definition	The enterprise's mission and business processes should address cybersecurity risks throughout the supply chain. When addressing mission and business process definitions, the enterprise should ensure that C-SCRM activities are incorporated into the support processes for achieving mission success. For example, a system supporting a critical mission function that has been designed and implemented for easy removal and replacement should a component fail may require the use of somewhat unreliable hardware components. A C-SCRM activity may need to be defined to ensure that the supplier makes component spare parts readily available if a replacement is needed.	Functional	Equal	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	10	a. Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes;
PM-12	Insider Threat Program	An insider threat program should include C-SCRM and be tailored for both federal and non-federal agency individuals who have access to agency systems and networks. This control applies to contractors and subcontractors and should be implemented throughout the SDLC.	Functional	Equal	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross-discipline insider threat incident handling team.	10	Implement an insider threat program that includes a cross-discipline insider threat incident handling team.
PM-26	Complaint Management	Complaint management process and mechanisms should be protected from cybersecurity risks throughout the supply chain. Enterprises should also integrate C-SCRM security and privacy controls when fielding complaints from vendors or the general public (e.g., departments and agencies fielding inquiries related to exclusions and removals).	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes: a. Mechanisms that are easy to use and readily accessible by the public; b. All information necessary for successfully filing complaints;
PM-26	Complaint Management	Complaint management process and mechanisms should be protected from cybersecurity risks throughout the supply chain. Enterprises should also integrate C-SCRM security and privacy controls when fielding complaints from vendors or the general public (e.g., departments and agencies fielding inquiries related to exclusions and removals).	Functional	Intersects With	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	5	Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes: a. Mechanisms that are easy to use and readily accessible by the public; b. All information necessary for successfully filing complaints;
PM-27	Privacy Reporting	Privacy reporting process and mechanisms should be protected from cybersecurity risks throughout the supply chain.	Functional	Equal	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	10	a. Develop [Assignment: organization-defined privacy reports] and disseminate to: 1. [Assignment: organization-defined oversight bodies] to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and 2. [Assignment: organization-defined officials] and other personnel with responsibility for monitoring
PM-31	Continuous Monitoring Strategy	The continuous monitoring strategy and program should integrate CSCRM controls at Levels 1, 2, and 3 in accordance with the Supply Chain Risk Management Strategy.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include: a. Establishing the following organization-wide metrics to be monitored: [Assignment: organization-defined metrics]; b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment:
PM-32	Purposing	Extending systems assigned to support specific mission or business functions beyond their initial purpose subjects those systems to unintentional risks, including cybersecurity risks throughout the supply chain. The application of this control should include the explicit incorporation of cybersecurity supply chain exposures.	Functional	Equal	Purpose Validation	GOV-11	Mechanisms exist to monitor mission/business-critical Technology Assets, Applications and/or Services (TAAS) to ensure those resources are being used consistent with their intended purpose.	10	Analyze [Assignment: organization-defined systems or systems components] supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.
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	The procedures can be established for the security and privacy program in general and individual information 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	The procedures can be established for the security and privacy program in general and individual information 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-1	Policy and Procedures	risk assessment should include both the supply chain infrastructure (e.g., development and testing environments and delivery systems) and the information system/components traversing the supply chain. System-level risk assessments significantly intersect with the SDLC and should complement the enterprise's broader RMF activities, which take part during the SDLC. A criticality analysis will ensure that mission-critical functions and components are given higher priority due to their impact on the mission, if compromised. The policy should include supply chainrelevant cybersecurity roles that are applicable to performing and coordinating risk assessments across the enterprise (see Section 2 for the listing and description of roles). Applicable roles within suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers should be	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
RA-1	Policy and Procedures	risk assessment should include both the supply chain infrastructure (e.g., development and testing environments and delivery systems) and the information system/components traversing the supply chain. System-level risk assessments significantly intersect with the SDLC and should complement the enterprise's broader RMF activities, which take part during the SDLC. A criticality analysis will ensure that mission-critical functions and components are given higher priority due to their impact on the mission, if compromised. The policy should include supply chainrelevant cybersecurity roles that are applicable to performing and coordinating risk assessments across the enterprise (see Section 2 for the listing and description of roles). Applicable roles within suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers should be	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
RA-1	Policy and Procedures	risk assessment should include both the supply chain infrastructure (e.g., development and testing environments and delivery systems) and the information system/components traversing the supply chain. System-level risk assessments significantly intersect with the SDLC and should complement the enterprise's broader RMF activities, which take part during the SDLC. A criticality analysis will ensure that mission-critical functions and components are given higher priority due to their impact on the mission, if compromised. The policy should include supply chainrelevant cybersecurity roles that are applicable to performing and coordinating risk assessments across the enterprise (see Section 2 for the listing and description of roles). Applicable roles within suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers should be	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
RA-2	Security Categorization	Security categorization is critical to C-SCRM at Levels 1, 2, and 3. In addition to [FIPS 199] categorization, security categorization for C-SCRM should be based on the criticality analysis that is performed as part of the SDLC. See Section 2 and [NISTIR 8179] for a detailed description of criticality analysis.	Functional	Equal	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	10	a. Categorize the system and information it processes, stores, and transmits; b. Document the security categorization results, including supporting rationale, in the security plan for the system; and c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.
RA-3	Risk Assessment	Risk assessments should include an analysis of criticality, threats, vulnerabilities, likelihood, and impact, as described in detail in Appendix C. The data to be reviewed and collected includes C-SCRM-specific roles, processes, and the results of system/component and services acquisitions, implementation, and integration. Risk assessments should be performed at Levels 1, 2, and 3. Risk assessments at higher levels should consist primarily of a synthesis of various risk assessments performed at lower levels and used for understanding the overall impact with the level (e.g., at the enterprise or mission/function levels). C-SCRM risk assessments should complement and inform risk assessments, which are performed as ongoing activities throughout the SDLC, and processes should be appropriately aligned with or integrated into ERM processes and governance.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	a. Conduct a risk assessment, including: 1. Identifying threats to and vulnerabilities in the system; 2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
RA-3	Risk Assessment	Risk assessments should include an analysis of criticality, threats, vulnerabilities, likelihood, and impact, as described in detail in Appendix C. The data to be reviewed and collected includes C-SCRM-specific roles, processes, and the results of system/component and services acquisitions, implementation, and integration. Risk assessments should be performed at Levels 1, 2, and 3. Risk assessments at higher levels should consist primarily of a synthesis of various risk assessments performed at lower levels and used for understanding the overall impact with the level (e.g., at the enterprise or mission/function levels). C-SCRM risk assessments should complement and inform risk assessments, which are performed as ongoing activities throughout the SDLC, and processes should be appropriately aligned with or integrated into ERM processes and governance.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	a. Conduct a risk assessment, including: 1. Identifying threats to and vulnerabilities in the system; 2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
RA-3(1)	Risk Assessment | Supply Chain Risk Assessment	a. Assess supply chain risks associated with [Assignment: organization-defined systems, system components, and system services]; andb. Update the supply chain risk assessment [Assignment: organization-defined frequency], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.	Functional	Equal	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	10	
RA-5	Vulnerability Monitoring and Scanning	Vulnerability monitoring activities should take place at all three levels of the enterprise. Scoping vulnerability 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 VDR. Enterprises should also consider establishing a separate notification channel for customers in cases where	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

FDE #	FDE Name	Focal Document Element (FDE) Description NIST SP 800-161 R1 Supplemental C-SCRM Guidance	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
RA-5	Vulnerability Monitoring and Scanning	vulnerability monitoring activities should take place at all three levels of the enterprise. Scoping vulnerability 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 VDR. Enterprises should also consider establishing a separate notification channel for customers in cases where	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-5(3)	Vulnerability Monitoring and Scanning | Breadth and Depth of Coverage	Enterprises that monitor the supply chain for vulnerabilities should express the breadth of monitoring based on the criticality and/or risk profile of the supplier or product/component and the depth of monitoring based on the level of the supply chain at which the monitoring takes place (e.g., sub-supplier). Where possible, a component inventory (e.g., hardware, software) may aid enterprises in capturing the breadth and depth of the products/components within their supply chain that may need to be monitored and scanned for vulnerabilities	Functional	Equal	Breadth / Depth of Coverage	VPM-06.2	Mechanisms exist to identify the breadth and depth of coverage for vulnerability scanning that define the system components scanned and types of vulnerabilities that are checked for.	10	Define the breadth and depth of vulnerability scanning coverage.
RA-5(6)	Vulnerability Monitoring and Scanning | Automated Trend Analyses	Enterprises should track trends in vulnerabilities to components within the supply chain over time. This information may help enterprises develop procurement strategies that reduce risk exposure density within the supply chain.	Functional	Equal	Trend Analysis	VPM-06.4	Automated mechanisms exist to compare the results of vulnerability scans over time to determine trends in system vulnerabilities.	10	Compare the results of multiple vulnerability scans using [Assignment: organization-defined automated mechanisms].
RA-7	Risk Response	Enterprises should integrate capabilities to respond to cybersecurity risks throughout the supply chain into the enterprise's overall response posture, ensuring that these responses are aligned to and fall within the boundaries of the enterprise's tolerance for risk. Risk response should include consideration of risk response identification, evaluation of alternatives, and risk response decision activities	Functional	Equal	Risk Response	RSK-06.1	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments; (2) Audits; and/or (3) Incidents.	10	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.
RA-9	Criticality Analysis	chain risk management activities. First, enterprises should complete a criticality analysis as part of the Frame step of the C-SCRM Risk Management Process. Then, findings generated in the Assess step activities (e.g., criticality analysis, threat analysis, vulnerability analysis, and mitigation strategies) update and tailor the criticality analysis. A symbiotic relationship exists between the criticality analysis and other Assess step activities in that they inform and enhance one another. For a 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].
RA-10	Threat Hunting	threats to their supply chain. This requires a collaborative effort between C-SCRM and other cyber defense-oriented functions within the enterprise. Threat hunting capabilities may also be provided via a shared services enterprise, especially when an enterprise lacks the resources to perform threat hunting activities themselves. Typical activities include information sharing with peer enterprises and actively consuming threat intelligence sources (e.g., like those available from Information Assurance and Analysis Centers [ISAC[and Information Assurance and Analysis Organizations [ISAO]). These activities can help identify and flag indicators of increased cybersecurity risks throughout the supply chain that may be of concern, such as cyber incidents, mergers and acquisitions, and Foreign Ownership, Control, or Influence (FOCI). Supply chain threat intelligence should seek out threats to the enterprise's suppliers, as well as information systems, system components, and the raw inputs that they provide. The	Functional	Equal	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	10	a. Establish and maintain a cyber threat hunting capability to: 1. Search for indicators of compromise in organizational systems; and 2. Detect, track, and disrupt threats that evade existing controls; and b. Employ the threat hunting capability [Assignment: organization-defined frequency].
SA-1	Policy and Procedures	considered for any and all procurements of products or services in which there may be an unacceptable risk of a supplied product or service contractor compromising the integrity, availability, or confidentiality of an enterprise's information. This initial assessment should occur during the acquisition planning phase and will be minimally informed by an identification and understanding of the criticality of the enterprise's mission functions, its high value assets, and the sensitivity of the information that may be accessible by the supplied product or service provider. In addition, enterprises should develop policies and procedures that address supply chain risks that may arise during contract performance, such as a change of ownership or control of the business or when actionable information is learned that indicates that a supplier or a product is a target of a supply chain threat. Supply chains	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
SA-1	Policy and Procedures	considered for any and all procurements of products or services in which there may be an unacceptable risk of a supplied product or service contractor compromising the integrity, availability, or confidentiality of an enterprise's information. This initial assessment should occur during the acquisition planning phase and will be minimally informed by an identification and understanding of the criticality of the enterprise's mission functions, its high value assets, and the sensitivity of the information that may be accessible by the supplied product or service provider. In addition, enterprises should develop policies and procedures that address supply chain risks that may arise during contract performance, such as a change of ownership or control of the business or when actionable information is learned that indicates that a supplier or a product is a target of a supply chain threat. Supply chains	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
SA-1	Policy and Procedures	considered for any and all procurements of products or services in which there may be an unacceptable risk of a supplied product or service contractor compromising the integrity, availability, or confidentiality of an enterprise's information. This initial assessment should occur during the acquisition planning phase and will be minimally informed by an identification and understanding of the criticality of the enterprise's mission functions, its high value assets, and the sensitivity of the information that may be accessible by the supplied product or service provider. In addition, enterprises should develop policies and procedures that address supply chain risks that may arise during contract performance, such as a change of ownership or control of the business or when actionable information is learned that indicates that a supplier or a product is a target of a supply chain threat. Supply chains	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
SA-3	System Development Life Cycle	There is a strong relationship between the SDLC and C-SCRM activities. The enterprise should ensure that C-SCRM activities are integrated into the SDLC for both the enterprise and for applicable suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. In addition to traditional SDLC activities, such as requirements and design, the SDLC includes activities such as inventory management, acquisition and procurement, and the logical delivery of systems and components. See Section 2 and Appendix C for further guidance on SDLC. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5	a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations; b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle; c. Identify individuals having information security
SA-3	System Development Life Cycle	There is a strong relationship between the SDLC and C-SCRM activities. The enterprise should ensure that C-SCRM activities are integrated into the SDLC for both the enterprise and for applicable suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. In addition to traditional SDLC activities, such as requirements and design, the SDLC includes activities such as inventory management, acquisition and procurement, and the logical delivery of systems and components. See Section 2 and Appendix C for further guidance on SDLC. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations; b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle; c. Identify individuals having information security
SA-4	Acquisition Process	development methods, techniques, or practices that may be relevant. Identify and specify C-SCRM evaluation criteria, to include the weighting of such criteria. 2. Enterprises should: a. Establish a plan for the acquisition of spare parts to ensure adequate supply, and execute the plan if or when applicable; b. Establish a plan for the acquisition of alternative sources of supply as may be necessary during continuity events or if/when a disruption to the supply chain occurs; c. Work with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service: a. Security and privacy functional requirements; b. Strength of mechanism requirements;
SA-4	Acquisition Process	development methods, techniques, or practices that may be relevant. Identify and specify C-SCRM evaluation criteria, to include the weighting of such criteria. 2. Enterprises should: a. Establish a plan for the acquisition of spare parts to ensure adequate supply, and execute the plan if or when applicable; b. Establish a plan for the acquisition of alternative sources of supply as may be necessary during continuity events or if/when a disruption to the supply chain occurs; c. Work with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service: a. Security and privacy functional requirements; b. Strength of mechanism requirements;
SA-4	Acquisition Process	development methods, techniques, or practices that may be relevant. Identify and specify C-SCRM evaluation criteria, to include the weighting of such criteria. 2. Enterprises should: a. Establish a plan for the acquisition of spare parts to ensure adequate supply, and execute the plan if or when applicable; b. Establish a plan for the acquisition of alternative sources of supply as may be necessary during continuity events or if/when a disruption to the supply chain occurs; c. Work with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service: a. Security and privacy functional requirements; b. Strength of mechanism requirements;
SA-4	Acquisition Process	development methods, techniques, or practices that may be relevant. Identify and specify C-SCRM evaluation criteria, to include the weighting of such criteria. 2. Enterprises should: a. Establish a plan for the acquisition of spare parts to ensure adequate supply, and execute the plan if or when applicable; b. Establish a plan for the acquisition of alternative sources of supply as may be necessary during continuity events or if/when a disruption to the supply chain occurs; c. Work with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	5	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service: a. Security and privacy functional requirements; b. Strength of mechanism requirements;
SA-4(5)	Acquisition Process | System, Component, and Service Configurations	If an enterprise needs to purchase components, they need to ensure that the product specifications are "fit for purpose" and meet the enterprise's requirements, whether purchasing directly from the OEM, channel partners, or a secondary market.	Functional	Equal	Pre-Established Secure Configurations	TDA-02.4	Mechanisms exist to ensure vendors / manufacturers: (1) Deliver the Technology Asset, Application and/or Service (TAAS) with a pre-established, secure configuration implemented; and (2) Use the pre-established, secure configuration as the default for any subsequent TAAS reinstallation or upgrade.	10	Require the developer of the system, system component, or system service to: (a) Deliver the system, component, or service with [Assignment: organization-defined security configurations] implemented; and (b) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.
SA-4(7)	Acquisition Process | NIAP-approved Protection Profiles	This control enhancement requires that the enterprise build, procure, and/or use U.S. Government protection profile-certified information assurance (IA) components when possible. NIAP certification can be achieved for OTS (COTS and GOTS)	Functional	Intersects With	Information Assurance Enabled Products	TDA-02.2	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-approved.	5	(a) Limit the use of commercially provided information assurance and information assurance-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; and (b) Require, if no NIAP-approved Protection Profile
SA-4(8)	Acquisition Process | Continuous Monitoring Plan for Controls	This control enhancement is relevant to C-SCRM and plans for continuous monitoring of control effectiveness and should therefore be extended to suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Equal	Continuous Monitoring Plan	TDA-09.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a plan for the continuous monitoring of security, compliance and/or resilience control effectiveness.	10	Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the organization.
SA-5	System Documentation	Information system documentation should include relevant C-SCRM concerns (e.g., C-SCRM plan). Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity.	Functional	Intersects With	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5	a. Obtain or develop administrator documentation for the system, system component, or system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security and privacy functions and mechanisms; and 3. Known vulnerabilities regarding configuration and
SA-5	System Documentation	Information system documentation should include relevant C-SCRM concerns (e.g., C-SCRM plan). Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity.	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	5	a. Obtain or develop administrator documentation for the system, system component, or system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security and privacy functions and mechanisms; and 3. Known vulnerabilities regarding configuration and
SA-8	Security and Privacy Engineering Principles	determined by risk assessments (see Section 2 and Appendix C). c. Document and gain management acceptance and approval for risk that is not fully mitigated. d. Limit the number, size, and privilege levels of critical elements. Using criticality analysis will aid in determining which elements or functions are critical. See criticality analysis in Appendix C and NISTIR 8179, Criticality Analysis Process Model: Prioritizing Systems and Components. e. Use security mechanisms that help to reduce opportunities to exploit supply chain cybersecurity vulnerabilities, such as encryption, access control, identity management, and malware or tampering discovery. f. Design information system components and elements to be difficult to disable (e.g., tamperproofing techniques),	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].
SA-8	Security and Privacy Engineering Principles	determined by risk assessments (see Section 2 and Appendix C). c. Document and gain management acceptance and approval for risk that is not fully mitigated. d. Limit the number, size, and privilege levels of critical elements. Using criticality analysis will aid in determining which elements or functions are critical. See criticality analysis in Appendix C and NISTIR 8179, Criticality Analysis Process Model: Prioritizing Systems and Components. e. Use security mechanisms that help to reduce opportunities to exploit supply chain cybersecurity vulnerabilities, such as encryption, access control, identity management, and malware or tampering discovery. f. Design information system components and elements to be difficult to disable (e.g., tamperproofing techniques),	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].
SA-9(1)	External System Services | Risk Assessments and Organizational Approvals	See Appendices C and D. Departments and agencies should refer to Appendix E and Appendix F to implement guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity	Functional	Equal	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	10	(a) Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and (b) Verify that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles].
SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	c. Cyber supply chain threats, vulnerabilities, and associated risks are identified and documented. d. Enterprise data and information integrity, confidentiality, and availability requirements are defined and shared with the system suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers as appropriate. e. The consequences of non-compliance with C-SCRM requirements and information system security requirements are defined and documented. f. There is a clear delineation of accountabilities, roles, and responsibilities between contractors when multiple disparate providers are engaged in supporting a system or mission and business function. g. The requirements detail service contract completion and what defines the end of the suppliers, developers	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].
SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	c. Cyber supply chain threats, vulnerabilities, and associated risks are identified and documented. d. Enterprise data and information integrity, confidentiality, and availability requirements are defined and shared with the system suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers as appropriate. e. The consequences of non-compliance with C-SCRM requirements and information system security requirements are defined and documented. f. There is a clear delineation of accountabilities, roles, and responsibilities between contractors when multiple disparate providers are engaged in supporting a system or mission and business function. g. The requirements detail service contract completion and what defines the end of the suppliers, developers	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].
SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	c. Cyber supply chain threats, vulnerabilities, and associated risks are identified and documented. d. Enterprise data and information integrity, confidentiality, and availability requirements are defined and shared with the system suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers as appropriate. e. The consequences of non-compliance with C-SCRM requirements and information system security requirements are defined and documented. f. There is a clear delineation of accountabilities, roles, and responsibilities between contractors when multiple disparate providers are engaged in supporting a system or mission and business function. g. The requirements detail service contract completion and what defines the end of the suppliers, developers	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].

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
SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	c. Cyber supply chain threats, vulnerabilities, and associated risks are identified and documented. d. Enterprise data and information integrity, confidentiality, and availability requirements are defined and shared with the system suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers as appropriate. e. The consequences of non-compliance with C-SCRM requirements and information system security requirements are defined and documented. f. There is a clear delineation of accountabilities, roles, and responsibilities between contractors when multiple disparate providers are engaged in supporting a system or mission and business function.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].
SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	d. Enterprise data and information integrity, confidentiality, and availability requirements are defined and shared with the system suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers as appropriate. e. The consequences of non-compliance with C-SCRM requirements and information system security requirements are defined and documented. f. There is a clear delineation of accountabilities, roles, and responsibilities between contractors when multiple disparate providers are engaged in supporting a system or mission and business function.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].
SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	d. Enterprise data and information integrity, confidentiality, and availability requirements are defined and shared with the system suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers as appropriate. e. The consequences of non-compliance with C-SCRM requirements and information system security requirements are defined and documented. f. There is a clear delineation of accountabilities, roles, and responsibilities between contractors when multiple disparate providers are engaged in supporting a system or mission and business function.	Functional	Intersects With	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	5	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].
SA-9(4)	External System Services | Consistent Interests of Consumers and Providers	In the context of this enhancement, "providers" may include suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Equal	Conflict of Interests	TPM-04.3	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	10	Take the following actions to verify that the interests of [Assignment: organization-defined external service providers] are consistent with and reflect organizational interests: [Assignment: organization-defined actions].
SA-9(5)	External System Services | Processing, Storage, and Service Location	The location may be under the control of the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Enterprises should assess C-SCRM risks associated with a given geographic location and apply an appropriate risk response, which may include defining locations that are or are not acceptable and ensuring that appropriate protections are in place to address associated C-SCRM risk.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].
SA-9(5)	External System Services | Processing, Storage, and Service Location	The location may be under the control of the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Enterprises should assess C-SCRM risks associated with a given geographic location and apply an appropriate risk response, which may include defining locations that are or are not acceptable and ensuring that appropriate protections are in place to address associated C-SCRM risk.	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	Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].
SA-9(5)	External System Services | Processing, Storage, and Service Location	The location may be under the control of the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Enterprises should assess C-SCRM risks associated with a given geographic location and apply an appropriate risk response, which may include defining locations that are or are not acceptable and ensuring that appropriate protections are in place to address associated C-SCRM risk.	Functional	Intersects With	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	5	Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].
SA-10	Developer Configuration Management	Developer configuration management is critical for reducing cybersecurity risks throughout the supply chain. By conducting configuration management activities, developers reduce the occurrence and likelihood of flaws while increasing accountability and ownership for the changes. Developer configuration management should be performed both by developers internal to federal agencies and integrators or external service providers. 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	Developer Configuration Management	TDA-14	Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation.	10	Require the developer of the system, system component, or system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal]; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined
SA-11	Developer Testing and Evaluation	determine whether the supplier (OEM) has performed such testing as part of their quality or security processes. When the acquirer has control over the application and development processes, they should require this testing as part of the SDLC. In addition to the specific types of testing activities described in the enhancements, examples of C-SCRM-relevant testing include testing for counterfeits, verifying the origins of components, examining configuration settings prior to integration, and testing interfaces. These types of tests may require significant resources and should be prioritized based on criticality, threat, and vulnerability analyses (described in Section 2 and Appendix C), as well as the effectiveness of testing techniques. Enterprises may also require third-party testing	Functional	Equal	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	10	Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to: a. Develop and implement a plan for ongoing security and privacy control assessments; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at
SA-15	Development Process, Standards, and Tools	enterprise should apply national and international standards and best practices when implementing this control. Using existing standards promotes consistency of implementation, reliable and defendable processes, and interoperability. The enterprise's development, maintenance, test, and deployment environments should all be covered by this control. The tools included in this control can be manual or automated. The use of automated tools aids thoroughness, efficiency, and the scale of analysis that helps address cybersecurity risks that arise in relation to the development process throughout the supply chain. Additionally, the output of such activities and tools provides useful inputs for C-SCRM processes, as described in Section 2 and Appendix C. This control has applicability to the internal enterprise's processes, information systems, and networks as well as applicable system	Functional	Equal	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	a. Require the developer of the system, system component, or system service to follow a documented development process that: 1. Explicitly addresses security and privacy requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool
SA-15(3)	Development Process, Standards, and Tools | Criticality Analysis	This enhancement identifies critical components within the information system, which will help determine the specific C-SCRM activities to be implemented for critical components. See C-SCRM Criticality Analysis described in Appendix C for additional context.	Functional	Equal	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).	10	Require the developer of the system, system component, or system service to perform a criticality analysis: (a) At the following decision points in the system development life cycle: [Assignment: organization-defined decision points in the system development life cycle]; and (b) At the following level of rigor: [Assignment:
SA-15(4)	Development Process, Standards, and Tools | Threat Modeling and Vulnerability Analysis	This enhancement provides threat modeling and vulnerability analysis for the relevant federal agency and contractor products, applications, information systems, and networks. Performing this analysis will help integrate C-SCRM into code refinement and modification activities. See the C-SCRM threat and vulnerability analyses described in Appendix C for additional context.	Functional	Equal	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	10	This control that exists within NIST SP 800-161 R1 was withdrawn from NIST 800-53 R5 and no longer exists.
SA-15(8)	Development Process, Standards, and Tools | Reuse of Threat and Vulnerability Information	This enhancement encourages developers to reuse the threat and vulnerability information produced by prior development efforts and lessons learned from using the tools to inform ongoing development efforts. Doing so will help determine the C-SCRM activities described in Section 2 and Appendix C.	Functional	Equal	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	10	Require the developer of the system, system component, or system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.
SA-16	Developer-provided Training	Developer-provided training for external and internal developers is critical to C-SCRM. It addresses training the individuals responsible for federal systems and networks to include applicable development environments. Developer-provided training in this control also applies to the individuals who select system and network components. Developer-provided training should include CSCRM material to ensure that 1) developers are aware of potential threats and vulnerabilities when developing, testing, and maintaining hardware and software, and 2) the individuals responsible for selecting system and network components incorporate C-SCRM when choosing such components. Developer training should also cover training for secure coding and the use of tools to find vulnerabilities in software. Refer to Appendix F for additional guidance on security for critical software.	Functional	Equal	Developer-Provided Training	TDA-16	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to provide training on the correct use and operation of the Technology Asset, Application and/or Service (TAAS).	10	Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: [Assignment: organization-defined training].
SA-17	Developer Security and Privacy Architecture and Design	This control facilitates the use of C-SCRM information to influence system architecture, design, and component selection decisions, including security functions. Examples include identifying components that compose system architecture and design or selecting specific components to ensure availability through multiple supplier or component selections. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity	Functional	Equal	Developer Architecture & Design	TDA-05	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that: (1) Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; (2) Accurately and completely describes the required security functionality and the allocation of security, compliance and resilience controls among physical	10	Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that: a. Is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture; b. Accurately and completely describes the required
SA-20	Customized Development of Critical Components	The enterprise may decide, based on their assessments of cybersecurity risks throughout the supply chain, that they require customized development of certain critical components. This control provides additional guidance on this activity. Enterprises should work with suppliers and partners to ensure that critical components are identified. Organizations should ensure that they have a continued ability to maintain custom-developed critical software components. For example, having the source code, build scripts, and tests for a software component could enable an organization to have someone else maintain it if necessary.	Functional	Equal	Customized Development of Critical Components	TDA-12	Mechanisms exist to custom-develop critical system components, when Commercial Off The Shelf (COTS) solutions are unavailable.	10	Reimplement or custom develop the following critical system components: [Assignment: organization-defined critical system components].
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-
SA-21(1)	Developer Screening | Validation of Screening	Internal developer screening should be validated. Enterprises may validate system integrator developer screening by requesting summary data from the system integrator to be provided post-validation.	Functional	Intersects With	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.	5	This control that exists within NIST SP 800-161 R1 was withdrawn from NIST 800-53 R5 and no longer exists.
SA-22	Unsupported System Components	and resellers reduces cybersecurity risks in the supply chain. In the case of unsupported system components, the enterprise should use authorized resellers or distributors with an ongoing relationship with the supplier of the unsupported system components. When purchasing alternative sources for continued support, enterprises should acquire directly from vetted original equipment manufacturers (OEMs) or their authorized distributors and resellers. Decisions about using alternative sources require input from the enterprise's engineering resources regarding the differences in alternative component options. For example, if an alternative is to acquire an open source software component, the enterprise should identify the open source community development, test, acceptance, and release processes. Departments and agencies should refer to Appendix F to implement this guidance in accordance with	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5	a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or b. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]].