Set Theory Relationship Mapping (STRM)

Reference Document : **Secure Controls Framework (SCF) version 2024.3**
Focal Document: **NIST SP 800-161 R1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations**
Focal Document Source: **https://csrc.nist.gov/pubs/sp/800/161/r1/final**
STRM URL: **https://securecontrolsframework.com/content/strm/scf-2024-3-nist-800-161-r1.pdf**

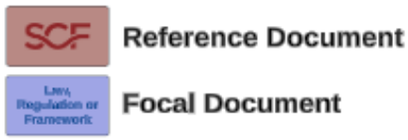
Set Theory Relationship Mapping (STRM) is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., cybersecurity & data privacy requirements). STRM also allows the strength of the mapping to be captured.

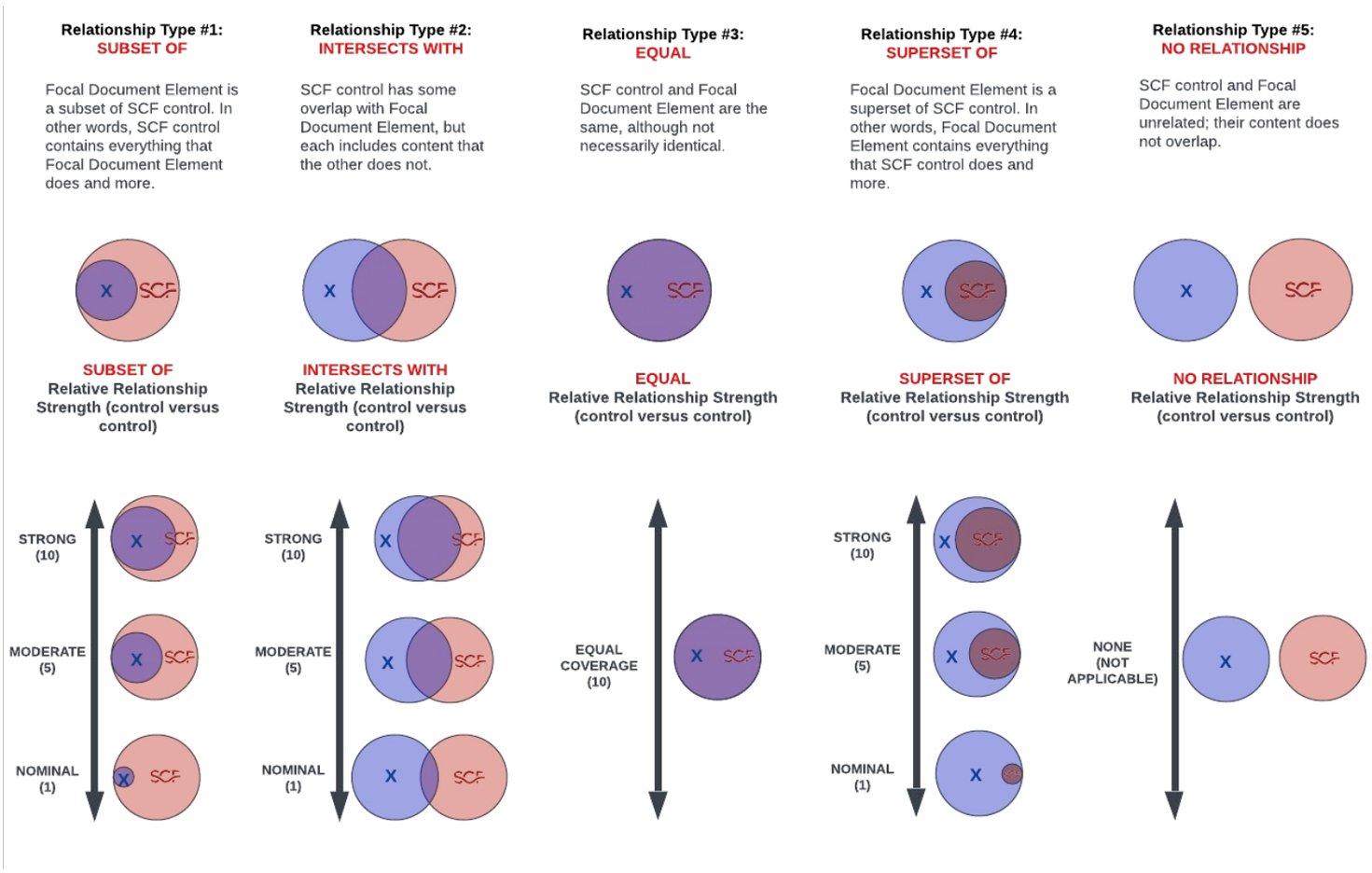
STRM relies on a justification for the relationship claim. There are three (3) options for the rationale, which is a high-level context within which the two concepts are related:

1. **Syntactic**: How similar is the wording that expresses the two concepts? This is a word-for-word analysis of the relationship, not an interpretation of the language.
2. **Semantic**: How similar are the meanings of the two concepts? This involves some interpretation of each concept's language.
3. **Functional**: How similar are the results of executing the two concepts? This involves understanding what will happen if the two concepts are implemented, performed, or otherwise executed.

Based on NIST IR 8477, STRM supports five (5) five relationship types to describe the logical similarity between two distinct concepts:

1. **Subset Of**
2. **Intersects With**
3. **Equal**
4. **Superset Of**
5. **No Relationship**





Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
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 Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
			Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
AC-2	Account Management	Use of this control helps establish traceability of actions and actors in the supply chain. This control also helps ensure access authorizations of actors in the supply chain is appropriate on a continuous basis. The enterprise may 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 should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	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	
			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	
			Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
			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	
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	
			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	
			Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
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	Functional	Equal	Revocation of Access Authorizations	IAC-20.6	Mechanisms exist to revoke logical and physical access authorizations.	10	
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 & data privacy attributes prior to releasing information to external systems.	10	
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 design, implement and review firewall and router configurations to restrict connections between untrusted networks and internal systems.	10	
AC-4(1)	Information Flow Enforcement | Metadata	The metadata relevant to C-SCRM is extensive and includes activities within the SDLC. For example, information about systems and system components, acquisition details, and delivery is considered metadata and may require appropriate protections. Enterprises should identify what metadata is directly relevant to their supply chain security and ensure that information flow enforcement is implemented in order to protect applicable metadata.	Functional	Equal	Object Security Attributes	NET-04.2	Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.	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	
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 privacy filters on metadata.	10	
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 systems, applications and services that protections from other network resources.	10	
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	
			Functional	Intersects With	Dual Authorization for Change	CHG-04.3	Mechanisms exist to enforce a two-person rule for implementing changes to critical assets.	5	
			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	
			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	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
AC-6	Least Privilege	For C-SCRM supplemental guidance, see control enhancements. 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	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
			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	
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	
AC-17	Remote Access	Ever more frequently, supply chains are accessed remotely. Whether for the purpose of development, maintenance, or the operation of information systems, enterprises should implement secure remote access mechanisms and allow remote access only to vetted personnel. Remote access to an enterprise's supply chain (including distributed software development environments) should be limited to the enterprise or contractor personnel and only if and as required to perform their tasks. Remote access requirements – such using a secure VPN, employing multi-factor authentication, or limiting access to specified business hours or from specified geographic locations – must be properly defined in agreements. Enterprises should require their prime contractors to implement this control and flow down this	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
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	
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	
			Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect wireless access via secure authentication and encryption.	5	
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 systems.	10	
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 Information Systems	DCH-13	Mechanisms exist to govern how external parties, systems and services are used to securely store, process and transmit data.	10	
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, systems and services from storing, processing and transmitting data unless authorized individuals first: ▪ Verifying the implementation of required security controls; or ▪ Retaining a processing agreement with the entity hosting the external systems or service.	10	
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 Systems / Components / Devices	DCH-13.4	Mechanisms exist to restrict the use of non-organizationally owned information systems, system components or devices to process, store or transmit organizational information.	10	
AC-21	Information Sharing	Sharing information within the supply chain can help manage cybersecurity risks throughout the supply chain. This information may include vulnerabilities, threats, the criticality of systems and components, or delivery information. This information sharing should be carefully managed to ensure that the information is only accessible to authorized individuals within the enterprise's supply chain. Enterprises should clearly define boundaries for information sharing with respect to temporal, informational, contractual, security, access, system, and other requirements. Enterprises should monitor and review for unintentional or intentional information sharing within its supply chain activities, including information sharing with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Intersects With	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	5	
			Functional	Intersects With	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5	
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	
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	
			Functional	Intersects With	Usage Restrictions of Sensitive Personal Data	PRI-05.4	Mechanisms exist to restrict the use of Personal Data (PD) to only the authorized purpose(s) consistent with applicable laws, regulations and in data privacy notices.	5	
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	
AT-1	Policy and Procedures	Enterprises should designate a specific official to manage the development, documentation, and dissemination of the training policy and procedures, including C-SCRM and role-based specific training for those with supply chain responsibilities. Enterprises should integrate cybersecurity supply chain risk management training and awareness into the security training and awareness policy. C-SCRM training should target both the enterprise and its contractors. The policy should ensure that supply chain cybersecurity role-based training is required for those individuals or functions that touch or impact the supply chain, such as the information system owner, acquisition, supply chain logistics, system engineering, program management, IT, quality, and incident response. C-SCRM training procedures should address: a. Roles throughout the supply chain and system/element life cycle to limit the opportunities and means available to individuals performing these roles that could result in adverse consequences, b. Requirements for interaction between an enterprise's personnel and individuals not employed by the enterprise who participate in the supply chain throughout the SDLC, and c. Incorporating feedback and lessons learned from C-SCRM activities into the C-SCRM training.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
			Functional	Subset Of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
			Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
AT-2	Literacy Training and Awareness	C-SCRM-specific supplemental guidance is provided in the control enhancements. 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	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
AT-2(1)	Literacy Training and Awareness | Practical Exercises	Enterprises should provide practical exercises in literacy training that simulate supply chain cybersecurity events and incidents. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-level contractors.	Functional	Intersects With	Simulated Cyber Attack Scenario Training	SAT-02.1	Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.	5	
AT-2(2)	Literacy Training and Awareness | Insider Threat	Enterprises should provide literacy training on recognizing and reporting potential indicators of insider threat within the supply chain. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Equal	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	10	
AT-2(3)	Literacy Training and Awareness | Social Engineering and Mining	Enterprises should provide literacy training on recognizing and reporting potential and actual instances of supply chain-related social engineering and social mining. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-level contractors.	Functional	Equal	Social Engineering & Mining	SAT-02.2	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.	10	
AT-2(4)	Literacy Training and Awareness | Suspicious Communications and Anomalous System Behavior	Provide literacy training on recognizing suspicious communications or anomalous behavior in enterprise supply chain systems. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-level contractors.	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	
AT-2(5)	Literacy Training and Awareness | Advanced Persistent Threat	Provide literacy training on recognizing suspicious communications on an advanced persistent threat (APT) in the enterprise's supply chain. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-level contractors.	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	
AT-2(6)	Literacy Training and Awareness | Cyber Threat Environment	Provide literacy training on cyber threats specific to the enterprise's supply chain environment. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-level contractors	Functional	Equal	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity & data privacy awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	10	
AT-3	Role-based Training	Addressing cyber supply chain risks throughout the acquisition process is essential to performing C-SCRM effectively. Personnel who are part of the acquisition workforce require training on what C-SCRM requirements, clauses, and evaluation factors are necessary to include when conducting procurement and how to incorporate C-SCRM into each acquisition phase. Similar enhanced training requirements should be tailored for personnel responsible for conducting threat assessments. Responding to threats and identified risks requires training in counterintelligence awareness and reporting. Enterprises should ensure that developers receive training on secure development practices as well as the use of vulnerability scanning tools. Enterprises should require their prime contractors to implement this control and	Functional	Intersects With	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: ▪ Before authorizing access to the system or performing assigned duties; ▪ When required by system changes; and ▪ Annually thereafter.	5	
AT-3(2)	Role-based Training | Physical Security Controls	C-SCRM is impacted by a number of physical security mechanisms and procedures within the supply chain, such as manufacturing, shipping, receiving, physical access to facilities, inventory management, and warehousing. Enterprise and system integrator personnel who provide development and operational support to the enterprise should receive training on how to handle these physical security mechanisms and on the associated cybersecurity risks throughout the supply chain.	Functional	Intersects With	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: ▪ Before authorizing access to the system or performing assigned duties; ▪ When required by system changes; and ▪ Annually thereafter.	5	
AT-3(8)	Role-based Training | Counterintelligence Training	Public sector enterprises should provide specialized counterintelligence awareness training that enables its resources to collect, interpret, and act upon a range of data sources that may signal a foreign adversary's presence in the supply chain. At a minimum, counterintelligence training should cover known red flags, key information sharing concepts, and reporting requirements.	Functional	Intersects With	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: ▪ Before authorizing access to the system or performing assigned duties; ▪ When required by system changes; and ▪ Annually thereafter.	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
			Functional	Equal	Counterintelligence Training	SAT-03.9	Mechanisms exist to provide specialized counterintelligence awareness training that enables personnel to collect, interpret and act upon a range of data sources that may signal the presence of a hostile actor.	10	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
			Functional	Intersects With	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
			Functional	Intersects With	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
AT-4	Training Records	Enterprises should maintain documentation for C-SCRM-specific training, especially with regard to key personnel in acquisitions and counterintelligence.	Functional	Equal	Cybersecurity & Data Privacy Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including basic cybersecurity & data privacy awareness training, ongoing awareness training and specific-system training.	10	
AU-1	Policy and Procedures	Enterprises must designate a specific official to manage the development, documentation, and dissemination of the audit and accountability policy and procedures to include auditing of the supply chain information systems and network. The audit and accountability policy and procedures should appropriately address tracking activities and their availability for other various supply chain activities, such as configuration management. Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers activities should not be included in such a policy unless those functions are performed within the acquirer's supply chain information systems and network. Audit and accountability policy procedures should appropriately address supplier audits as a way to examine the quality of a particular supplier and the risk they present to the enterprise and the enterprise's supply chain.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
			Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
AU-2	Event Logging	An observable occurrence within the information system or supply chain network should be identified as a supply chain auditable event based on the enterprise's SDLC context and requirements. Auditable events may include 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 to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Reviews & Updates	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
			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	
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 systems to produce event logs that contain sufficient information to, at a minimum: ▪ Establish what type of event occurred; ▪ When (date and time) the event occurred; ▪ Where the event occurred; ▪ The source of the event; ▪ The outcome (success or failure) of the event; and	10	
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	
			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	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
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	
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	
AU-10(1)	Non-repudiation | Association of Identities	This enhancement helps traceability in the supply chain and facilitates the accuracy 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	
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	
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	
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	
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	Functional	Equal	Monitoring For Information Disclosure	MON-11	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of non-public information.	10	
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: ▪ Capture and log all content related to a user session; and ▪ Remotely view all content related to an established user session in real time.	10	
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	
AU-16(2)	Cross-organizational Audit Logging | Sharing of Audit Information	Whether managing a distributed audit environment or an audit datasharing environment between enterprises and 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	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	
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 cybersecurity & data privacy assessment and authorization controls.	10	
			Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
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 Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	
			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 cybersecurity & data privacy controls.	5	
			Functional	Intersects With	Cybersecurity & Data Privacy In Project Management	PRM-04	Mechanisms exist to assess cybersecurity & data privacy 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	
			Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity & data privacy controls in systems, applications and services 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	
			Functional	Intersects With	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements.	5	
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: ▪ Statutory, regulatory and contractual compliance obligations; ▪ Monitoring capabilities; ▪ Mobile devices; ▪ Databases; ▪ Application security; ▪ Embedded technologies (e.g., IoT, OT, etc.);	5	
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 Assessments	IAO-02.3	Mechanisms exist to accept and respond to the results of external assessments that are performed by impartial, external organizations.	10	
CA-3	Information Exchange	The exchange of information or data between the system and other systems requires scrutiny from a supply chain perspective. This includes understanding the interface characteristics and connections of those components/systems that are directly interconnected or the data that is shared through those components/systems with developers, system integrators, external system service providers, other ICT/OT-related service providers, and – in some cases – suppliers. Proper servicelevel agreements should be in place to ensure compliance to system information exchange requirements defined by the enterprise, as the transfer of information between systems in different security or privacy domains with different security or privacy policies introduces the risk that such transfers violate one or more domain security or	Functional	Intersects With	System Interconnections	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, the interface characteristics, cybersecurity & data privacy requirements and the nature of the information communicated.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
CA-5	Plan of Action and Milestones	For a system-level plan of actions and milestones (POA&Ms), enterprises need to ensure that a separate POA&M 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	Functional	Intersects With	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
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 systems, projects and services are officially authorized prior to "go live" in a production environment.	10	
CA-7	Continuous Monitoring	For C-SCRM-specific guidance on this control, see Section 2 of this publication. 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	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
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	
CM-1	Policy and Procedures	Configuration management impacts nearly every aspect of the supply chain. Configuration management is critical 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 service providers, and other ICT/OT-related service providers regarding the configuration management policy.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
			Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
			Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
CM-2	Baseline Configuration	Enterprises should establish a baseline configuration of both the information system and the development environment, including documenting, formally reviewing, and securing the agreement of stakeholders. The purpose 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 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	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: ▪ At least annually; ▪ When required due to so; or ▪ As part of system component installations and upgrades.	5	
			Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
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	
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	
			Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
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	
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 cybersecurity and/or data privacy controls following implemented changes to ensure applicable controls operate as designed.	5	
			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	
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	Cybersecurity & Data Privacy Representative for Asset Lifecycle Changes	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data privacy representative in the configuration change control review process.	10	
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	
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	
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 systems.	10	
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 systems.	5	
			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	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
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	
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	
CM-6	Configuration Settings	Enterprises should oversee the function of modifying configuration settings for their 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	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
			Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	5	
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 systems through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
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	
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	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	
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	
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	
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	
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 Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	
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 Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	
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	
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 Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	
CM-8	System Component Inventory	Enterprises should ensure that critical component assets within the information systems and networks are included in the asset inventory. The inventory must also include information for critical component accountability. 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, including purchased software, open source software, and in-house software. Departments and agencies should refer to Appendix F for additional guidance on SBOMs 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 that: ▪ Accurately reflects the current systems, applications and services in use; ▪ Identifies authorized software products, including business justification details; ▪ Is at the level of granularity deemed necessary for tracking and reporting; ▪ Includes organization-defined information deemed necessary to achieve effective property accountability; and	5	
			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	
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	
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	
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	
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	
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,	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	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
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	
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	
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.
			Functional	Intersects With	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for systems that describe: ▪ Secure configuration, installation and operation of the system; ▪ Effective use and maintenance of security features/functions; and ▪ 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.
			Functional	Intersects With	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security controls to be utilized within systems, system components or services 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.
			Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate a Software Bill of Materials (SBOM) for systems, applications and services 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.
			Functional	Intersects With	Developer Architecture & Design	TDA-05	Mechanisms exist to require the developers of systems, system components or services to produce a design specification and security architecture that: ▪ 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; ▪ Accurately and completely describes the required security functionality and the allocation of security controls among physical and logical	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	
			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	
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	
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	
CM-10(1)	Software Usage Restrictions | Open-source Software	When considering software, enterprises should review all options and corresponding risks, including open source or commercially licensed components. When using open source software (OSS), the enterprise should understand and review the open source community's typical procedures regarding provenance, configuration management, sources, binaries, reusable 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:	Functional	Equal	Open Source Software	CFG-04.1	Mechanisms exist to establish parameters for the secure use of open source software.	10	
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	
			Functional	Intersects With	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	
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	
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 cybersecurity & data privacy controls are in place to protect organizational information and individual data privacy.	10	
CM-13	Data Action Mapping	In addition to personally identifiable information, understanding and documenting a map of system data actions for 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	Functional	Equal	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of technology assets where sensitive/regulated data is stored, transmitted or processed.	10	
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	
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 Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
			Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
			Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
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 assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
			Functional	Intersects With	Ongoing Contingency Planning	BCD-06	Mechanisms exist to keep contingency plans current with business needs, technology changes and feedback from contingency plan testing activities.	5	
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	
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	
CP-2(7)	Contingency Plan | Coordinate with External Service Providers	Enterprises should ensure that the supply chain network, information systems, and components provided by an 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	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	
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 systems, applications and services that support essential missions and business functions.	10	
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	
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	
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	
			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	
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	
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 Site	BCD-08.1	Mechanisms exist to separate the alternate storage site from the primary storage site to reduce susceptibility to similar threats.	10	
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	
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	
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	
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	
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	
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 Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
			Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
			Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
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	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	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
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	
IA-4	Identifier Management	Identifiers allow for greater discoverability and traceability. Within the enterprise's supply chain, identifiers should be assigned to systems, individuals, documentation, devices, and components. In some cases, identifiers may be maintained throughout a system's life cycle – from concept to retirement – but, at a minimum, throughout the 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 should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	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	
			Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and systems.	5	
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	
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 securely manage authenticators for users and devices.	5	
			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	
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	
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	
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	
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	Functional	Equal	Identification & Authentication for Third Party Systems & Services	IAC-05	Mechanisms exist to identify and authenticate third-party systems and services.	10	
IR-1	Policy and Procedures	Enterprises should integrate C-SCRM into incident response policy and procedures, and related C-SCRM Strategy/Implementation Plans and Policies. The policy and procedures must provide direction for how to address supply chain-related incidents and cybersecurity incidents that may complicate or impact the supply chain. Individuals who work within specific mission and system environments need to recognize cybersecurity supply chain-related incidents. The incident response policy should state when and how threats and incidents should be handled, reported, and managed. Additionally, the policy should define when, how, and with whom to communicate to the FASC (Federal Acquisition Security Council) and other stakeholders or partners within the broader supply chain in the event of a cyber threat or incident. Departments and agencies must notify the FASC of supply chain risk information when the FASC requests information relating to a particular source, covered article, or procures or an executive agency has determined that there is a reasonable basis to conclude a substantial supply chain risk associated with a source, covered procurement, or covered article exists. In such instances, the executive agency shall provide the FASC with relevant information concerning the source or covered article, including 1) the supply chain risk information identified through the course of the agency's activities in furtherance of mitigating, identifying, or managing its supply chain risk and 2) the supply chain risk information regarding covered procurement actions by the agency under the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) 41 U.S.C. § 4713; and any orders issued by the agency under 41 U.S.C. § 4713. Bidirectional communication with supply chain partners should be defined in agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to inform all involved parties of a supply chain cybersecurity incident. Incident information may also be shared with enterprises such as the Federal Bureau of Investigation (FBI), US CERT (United States Computer Emergency Readiness Team), and the NCCIC (National Cybersecurity and Communications Integration Center) as appropriate. Depending on the severity of the incident, the need for accelerated communications up and down the supply chain may be necessary. Appropriate agreements should be put in place with suppliers, developers, system integrators, external system service providers, and other ICT/OTrelated service providers to ensure speed of communication, response, corrective actions, and other related activities. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. In Level 2 and Level 3, procedures and enterprise-specific incident response methods must be in place, training completed (consider including Operations Security [OPSEC] and any appropriate threat briefing in training), and coordinated communication established throughout the supply chain to ensure an efficient and coordinated incident response effort.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			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 & data privacy-related incidents.	10	
			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	
			Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	5	
			Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
IR-1(1)	Policy and Procedures | C-SCRM Incident Information Sharing	Enterprises should ensure that their incident response policies and procedures provide guidance on effective information sharing of incidents and other key risk indicators in the supply chain. Guidance should – at a minimum – cover the collection, synthesis, and distribution of incident information from a diverse set of data sources, such as public data repositories, paid subscription services, and in-house threat intelligence teams. Enterprises that operate in the public sector should include specific guidance on when and how to communicate with interagency partnerships, such as the FASC (Federal Acquisition Security Council) and other stakeholders or partners within the broader supply chain, in the event of a cyber threat or incident. Departments and agencies must notify the FASC of supply chain risk information when: 1) The FASC requests information relating to a particular source or covered article, or 2) An executive agency has determined that there is a reasonable basis to conclude that a substantial supply chain risk associated with a source, covered procurement, or covered article exists. In such instances, the executive agency shall provide the FASC with relevant information concerning the source or	Functional	Intersects With	Correlation with External Organizations	IRO-02.5	Mechanisms exist to coordinate with approved third-parties to achieve a cross-organization perspective on incident awareness and more effective incident responses.	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
			Functional	Intersects With	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity & data privacy incident information to the provider of the product or service and other organizations involved in the supply chain for systems or system components related to the incident.	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
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	
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	
IR-4	Incident Handling	Suspected cybersecurity supply chain events that may trigger an organization's C-SCRM incident handling processes. Refer to Appendix G: Task 3.4 for examples of supply chain events. C-SCRM-specific supplemental guidance is provided in control enhancements.	Functional	Equal	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	10	
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	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
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	
IR-4(10)	Incident Handling | Supply Chain Coordination	A number of enterprises may be involved in managing incidents and responses for supply chain security. After initially processing the incident and deciding on a course of action (in some cases, the action may be "no action"), the enterprise may need to coordinate with their suppliers, developers, system integrators, external system service providers, other ICT/OT-related service providers, and any relevant interagency bodies to facilitate communications, incident response, root cause, and corrective actions. Enterprises should securely share information through a coordinated set of personnel in key roles to allow for a more comprehensive incident handling approach. Selecting suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers with mature capabilities for supporting supply chain cybersecurity incident handling is important for reducing exposure to cybersecurity risks throughout the supply chain. If transparency for incident handling is limited due to the nature of the relationship, define a set of acceptable criteria in the agreement (e.g., contract). A review (and potential revision) of the agreement is recommended, based on the lessons learned from previous incidents. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	
			Functional	Intersects With	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity & data privacy incident information to the provider of the product or service and other organizations involved in the supply chain for systems or system components related to the incident.	5	
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 & data privacy incident response operations.	10	
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 & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	10	
IR-6	Incident Reporting	C-SCRM-specific supplemental guidance provided in control enhancement IR-6 (3).	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: ▪ Internal stakeholders; ▪ Affected clients & third-parties; and ▪ Regulatory authorities.	5	
			Functional	Intersects With	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	5	
			Functional	Intersects With	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	5	
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 & data privacy incident information to the provider of the product or service and other organizations involved in the supply chain for systems or system components related to the incident.	5	
IR-7	Incident Response Assistance	C-SCRM-specific supplemental guidance provided in control enhancement IR-7 (2).	Functional	Equal	Incident Reporting Assistance	IRO-11	Mechanisms exist to provide incident response advice and assistance to users of systems for the handling and reporting of actual and potential cybersecurity & data privacy incidents.	10	
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	
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	
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	Information Spillage Response	IRO-12	Mechanisms exist to respond to sensitive information spills.	5	
			Functional	Intersects With	Responsible Personnel	IRO-12.1	Mechanisms exist to formally assign personnel or roles with responsibility for responding to sensitive information spills.	5	
MA-1	Policy and Procedures	Enterprises should ensure that C-SCRM is included in maintenance policies and procedures and any related SCRM Strategy/Implementation Plan, SCRM Policies, and SCRM Plan(s) for all enterprise information systems and networks. With many maintenance contracts, information on mission-, enterprise-, and system-specific objectives and requirements is shared between the enterprise and its suppliers, developers, system integrators, external system service providers, and other ICT/OTrelated service providers, allowing for vulnerabilities and opportunities for attack. In many cases, the maintenance of systems is outsourced to a system integrator, and as such, appropriate measures must be taken. Even when maintenance is not outsourced, the supply chain affects 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. Maintenance policies should be refined and augmented at each level. At Level 1, the policy should explicitly assert that C-SCRM should be applied throughout the SDLC, including maintenance activities. At Level 2, the policy should reflect the mission operation's needs and critical functions. At Level 3, it should reflect the specific system needs. The requirements in Level 1, such as nonlocal maintenance, should flow to Level 2 and Level 3. For example, when nonlocal maintenance is not allowed by Level 1, it should also not be allowed at Level 2 or Level 3. The enterprise should communicate applicable maintenance policy requirements to relevant prime contractors and require that they implement this control and flow down this requirement to relevant sub-tier contractors.	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	
			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	
			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	
			Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
			Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
MA-2	Controlled Maintenance	C-SCRM-specific supplemental guidance is provided in control enhancement MA-2 (2).	Functional	Equal	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the system, application or service.	10	
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	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
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,	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5	
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	
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	
MA-3(3)	Maintenance Tools | Prevent Unauthorized Removal	The unauthorized removal of systems and network maintenance tools from the supply chain may introduce supply 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	Functional	Equal	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that containing organizational information.	10	
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	
			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	
			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	
MA-4(3)	Nonlocal Maintenance | Comparable Security and Sanitization	Should 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	Functional	Equal	Remote Maintenance Comparable Security & Sanitization	MNT-05.6	Mechanisms exist to require systems performing remote, non-local maintenance and / or diagnostic services implement a security capability comparable to the capability implemented on the system being serviced.	10	
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	
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	
MA-6	Timely Maintenance	The enterprise should purchase spare parts, replacement parts, or alternative sources through original equipment manufacturers (OEMs), authorized distributors, 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	Functional	Equal	Timely Maintenance	MNT-03	Mechanisms exist to obtain maintenance support and/or spare parts for systems within a defined Recovery Time Objective (RTO).	10	
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	
MA-8	Maintenance Monitoring and Information Sharing	Tracking the failure rates of components provides useful 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 technical alternatives.	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.
			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-1	Policy and Procedures	Various documents and information on a variety of physical and electronic media are disseminated throughout the supply chain. This information may contain a variety of sensitive information and intellectual property from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers and should be appropriately protected. Media protection policies and procedures should also address supply chain concerns, including media in the enterprise's supply chain and throughout the SDLC.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
			Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
			Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
MP-4	Media Storage	Media storage controls should include C-SCRM activities. Enterprises should specify and include in agreements (e.g., contracting language) media storage requirements (e.g., encryption) for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The enterprise should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Equal	Media Storage	DCH-06	Mechanisms exist to: ▪ Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and ▪ Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	10	
MP-5	Media Transport	The enterprise should incorporate C-SCRM activities when media is transported by enterprise or non-enterprise personnel. Some of the techniques to protect media during transport and storage include cryptographic techniques and approved custodian services.	Functional	Equal	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	10	
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	
			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	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
		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	
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 Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
			Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
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	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	
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	
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	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	
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 Information Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical information systems or sensitive/regulated data, in addition to the physical access controls for the facility.	10	
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	
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	
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	
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	
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	
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	
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	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	
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-level contractors.	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	
			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	
			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	
			Functional	Intersects With	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.	5	
			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	
			Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
PL-1	Policy and Procedures	The security planning policy and procedures should integrate C-SCRM. This includes creating, disseminating, and updating the security policy, operational policy, and procedures for C-SCRM to shape acquisition or development requirements and the follow-on implementation, operations, and maintenance of systems, system interfaces, and network connections. The C-SCRM policy and procedures provide inputs into and take guidance from the C-SCRM Strategy and Implementation Plan at Level 1 and the System Security Plan and C-SCRM plan at Level 3. In Level 3, ensure that the full SDLC is covered from the C-SCRM perspective.	Functional	Subset Of	Cybersecurity & Data Privacy Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	10	
			Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
			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	
			Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
			Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
PL-2	System Security and Privacy Plans	The system security plan (SSP) should integrate C-SCRM. The enterprise may choose to develop a stand-alone C-SCRM plan for an individual system or integrate SCRM controls into their SSP. The system security plan and/or system-level C-SCRM plan provide inputs into and take guidance from the C-SCRM Strategy and Implementation 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) systems that are processing federal agency information and flow down this requirement to relevant sub-level contractors. Section 2, Appendix C, and Appendix D provide guidance on C-SCRM strategies, policies, and plans. Controls in this publication (NIST SP 800-161, Rev. 1) should be used for the C-SCRM portion of the SSP.	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	
			Functional	Intersects With	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	5	
			Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: • Contain sufficient detail to assess the security of the network's architecture; • Reflect the current architecture of the network environment; and • Document all sensitive/regulated data flows.	5	
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 & data privacy principles in their daily work.	5	
			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	
			Functional	Intersects With	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	
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	
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 cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
PL-8(2)	Security and Privacy Architectures | Supplier Diversity	Supplier diversity provides options for addressing information security and supply chain concerns. The enterprise should incorporate this control as it relates to suppliers, developers, system integrators, external system service 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,	Functional	Intersects With	Supplier Diversity	TDA-03.1	Mechanisms exist to obtain cybersecurity & data privacy technologies from different suppliers to minimize supply chain risk.	5	
PL-9	Central Management	C-SCRM controls are managed centrally at Level 1 through the CSCRM Strategy and Implementation Plan and at Level 1 and Level 2 through the C-SCRM Policy. The C-SCRM PMO described in Section 2 centrally manages C-SCRM controls at Level 1 and Level. At Level 3, C-SCRM controls are managed on an information system basis though the SSP and/or CSCRM Plan.	Functional	Intersects With	Centralized Management of Cybersecurity & Data Privacy Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of cybersecurity & data privacy controls and related processes.	5	
			Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	
			Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
			Functional	Intersects With	Centralized Management of Antimalware Technologies	END-04.3	Mechanisms exist to centrally-manage antimalware technologies.	5	
			Functional	Intersects With	Central Management	END-08.1	Mechanisms exist to centrally-manage anti-phishing and spam protection technologies.	5	
			Functional	Intersects With	Centralized Management of Planned Audit Record Content	MON-03.6	Mechanisms exist to centrally manage and configure the content required to be captured in audit records generated by organization-defined information system components.	5	
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	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
PM-2	Information Security Program Leadership Role	The senior information security officer (e.g., CISO) and senior agency official responsible for acquisition (e.g., Chief Acquisition Officer [CAO] or Senior Procurement Executive [SPE]) have key responsibilities for C-SCRM and the overall cross-enterprise coordination and collaboration with other applicable senior personnel within the enterprise, such as the CIO, the head of facilities/physical security, and the risk executive (function). This coordination should occur regardless of the specific department and agency enterprise structure and specific titles of relevant senior personnel. The coordination could be executed by the C-SCRM PMO or another similar function. Section 2 provides more guidance on C-SCRM roles and responsibilities.	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
PM-3	Information Security and Privacy Resources	An enterprise's C-SCRM program requires dedicated, sustained funding and human resources to successfully implement agency C-SCRM requirements. Section 3 of this document provides guidance on dedicated funding for C-SCRM programs. The enterprise should also integrate CSCRM requirements into major IT investments to ensure that funding is appropriately allocated through the capital planning and investment request process. For example, should an RFID infrastructure be required to enhance C-SCRM to secure and improve the inventory or logistics management efficiency of the enterprise's supply chain, appropriate IT investments would likely be required to ensure successful planning and implementation. Other examples include any investment into the development or test	Functional	Equal	Cybersecurity & Data Privacy Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity & data privacy programs and document all exceptions to this requirement.	10	
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	
			Functional	Intersects With	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
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	
			Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: ▪ Accurately reflects the current systems, applications and services in use; ▪ Identifies authorized software products, including business justification details; ▪ Is at the level of granularity deemed necessary for tracking and reporting; ▪ Includes organization-defined information deemed necessary to achieve effective property accountability; and	5	
PM-6	Measures of Performance	Enterprises should use measures of performance to track the implementation, efficiency, effectiveness, and impact of C-SCRM activities. The C-SCRM PMO is responsible for creating C-SCRM measures of performance in collaboration with other applicable stakeholders to include identifying the appropriate audience and decision makers and providing guidance on data collection, analysis, and reporting.	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
			Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
PM-7	Enterprise Architecture	C-SCRM should be integrated when designing and maintaining enterprise architecture.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
PM-8	Critical Infrastructure Plan	C-SCRM should be integrated when developing and maintaining critical infrastructure plan	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
			Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
PM-9	Risk Management Strategy	The risk management strategy should address cybersecurity risks throughout the supply chain. Section 2, Appendix C, and Appendix D of this document provide guidance on integrating C-SCRM into the risk management strategy.	Functional	Equal	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
PM-10	Authorization Process	C-SCRM should be integrated when designing and implementing authorization processes.	Functional	Equal	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	10	
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 cybersecurity & data privacy that determines: ▪ The resulting risk to organizational operations, assets, individuals and other organizations; and ▪ 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	
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	
PM-13	Security and Privacy Workforce	Security and privacy workforce development and improvement should ensure that relevant C-SCRM topics are integrated into the content and initiatives produced by the program. Section 2 provides information on C-SCRM roles and responsibilities. NIST SP 800-161 can be used as a source of topics and activities to include in the security and privacy workforce program.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
			Functional	Intersects With	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
PM-14	Testing, Training, and Monitoring	The enterprise should implement a process to ensure that organizational plans for conducting supply chain risk testing, training, and monitoring activities associated with organizational systems are maintained. The C-SCRM PMO can provide guidance and support on how to integrate C-SCRM into testing, training, and monitoring plans.	Functional	Intersects With	Testing, Training & Monitoring	PRI-08	Mechanisms exist to conduct cybersecurity & data privacy testing, training and monitoring activities	5	
			Functional	Intersects With	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
PM-15	Security and Privacy Groups and Associations	Contact with security and privacy groups and associations should include C-SCRM practitioners and those with C-SCRM responsibilities. Acquisition, legal, critical infrastructure, and supply chain groups and associations should be incorporated. The C-SCRM PMO can help identify agency personnel who could benefit from participation, specific groups to participate in, and relevant topics.	Functional	Intersects With	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	
			Functional	Intersects With	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the cybersecurity & data privacy communities to: ▪ Facilitate ongoing cybersecurity & data privacy education and training for organizational personnel; ▪ Maintain currency with recommended cybersecurity & data privacy practices, techniques and technologies; and ▪ Share current cybersecurity and/or data privacy-related information	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
PM-16	Threat Awareness Program	A threat awareness program should include threats that emanate from the supply chain. When addressing supply chain threat awareness, knowledge should be shared between stakeholders within the boundaries of the enterprise's information sharing policy. The C-SCRM PMO can help identify C-SCRM stakeholders to include in threat information sharing, as well as potential sources of information for supply chain threats.	Functional	Intersects With	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	
PM-17	Protecting Controlled Unclassified Information on External Systems	The policy and procedures for controlled unclassified information (CUI) on external systems should include protecting relevant supply chain information. Conversely, it should include protecting agency information that resides in external systems because such external systems are part of the agency supply chain.	Functional	Equal	Protecting Sensitive Data on External Systems	DCH-13.3	Mechanisms exist to ensure that the requirements for the protection of sensitive information processed, stored or transmitted on external systems, are implemented in accordance with applicable statutory, regulatory and contractual obligations.	10	
PM-18	Privacy Program Plan	The privacy program plan should include C-SCRM. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtier contractors.	Functional	Equal	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data privacy controls.	10	
PM-19	Privacy Program Leadership Role	The privacy program leadership role should be included as a stakeholder in applicable C-SCRM initiatives and activities.	Functional	Equal	Chief Privacy Officer (CPO)	PRI-01.1	Mechanisms exist to appoints a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement, applicable data privacy requirements and manage data privacy risks through the organization-wide data privacy program.	10	
PM-20	Dissemination of Privacy Program Information	The dissemination of privacy program information should be protected from cybersecurity risks throughout the supply chain.	Functional	Equal	Dissemination of Data Privacy Program Information	PRI-01.3	Mechanisms exist to: ▪ Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role; ▪ Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories; ▪ Utilize publicly facing email addresses and/or phone lines to enable the	10	
PM-21	Accounting of Disclosures	An accounting of disclosures should be protected from cybersecurity risks throughout the supply chain.	Functional	Equal	Accounting of Disclosures	PRI-14.1	Mechanisms exist to develop and maintain an accounting of disclosures of Personal Data (PD) held by the organization and make the accounting of disclosures available to the person named in the record, upon request.	10	
PM-22	Personally Identifiable Information Quality Management	Personally identifiable information (PII) quality management should take into account and manage cybersecurity risks related to PII throughout the supply chain.	Functional	Intersects With	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	5	
			Functional	Intersects With	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.	5	
PM-23	Data Governance Body	Data governance body is a stakeholder in C-SCRM and should be included in cross-agency collaboration and information sharing of C-SCRM activities and initiatives (e.g., by participating in inter-agency bodies, such as the FASC).	Functional	Intersects With	Data Management Board	PRI-13	Mechanisms exist to establish a written charter for a Data Management Board (DMB) and assigned organization-defined roles to the DMB.	5	
			Functional	Intersects With	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	5	
			Functional	Intersects With	Data Governance	GOV-10	Mechanisms exist to facilitate data governance to oversee the organization's policies, standards and procedures so that sensitive/regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.	5	
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	Supply chain-related cybersecurity risks to personally identifiable information should be addressed by the minimization policies and procedures described in this control.	Functional	Intersects With	Usage Restrictions of Sensitive Personal Data	PRI-05.4	Mechanisms exist to restrict the use of Personal Data (PD) to only the authorized purpose(s) consistent with applicable laws, regulations and in data privacy notices.	5	
			Functional	Intersects With	Collection Minimization	END-13.3	Mechanisms exist to utilize sensors that are configured to minimize the collection of information about individuals.	5	
			Functional	Intersects With	Minimize Visitor Personal Data (PD)	PES-06.5	Mechanisms exist to minimize the collection of Personal Data (PD) contained in visitor access records.	5	
			Functional	Intersects With	Internal Use of Personal Data For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: ▪ Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and ▪ Authorizes the use of PD when such information is required for internal testing, training and research.	5	
			Functional	Intersects With	Limit Personal Data (PD) Elements In Testing, Training & Research	DCH-18.2	Mechanisms exist to minimize the use of Personal Data (PD) for research, testing, or training, in accordance with the Data Protection Impact Assessment (DPIA).	5	
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 implement a process for receiving and responding to complaints, concerns or questions from data subjects about the organizational data privacy practices.	5	
			Functional	Intersects With	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to provide an organization-defined process for data subjects to appeal an adverse decision and have incorrect information amended.	5	
PM-27	Privacy Reporting	Privacy reporting process and mechanisms should be protected from cybersecurity risks throughout the supply chain.	Functional	Equal	Data Privacy Records & Reporting	PRI-14	Mechanisms exist to maintain data privacy-related records and develop, disseminate and update reports to internal senior management, as well as external oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory data privacy program mandates.	10	
PM-28	Risk Framing	C-SCRM should be included in risk framing. Section 2 and Appendix C provide detailed guidance on integrating C-SCRM into risk framing.	Functional	Equal	Risk Framing	RSK-01.1	Mechanisms exist to identify: ▪ Assumptions affecting risk assessments, risk response and risk monitoring; ▪ Constraints affecting risk assessments, risk response and risk monitoring; ▪ The organizational risk tolerance; and ▪ Priorities, benefits and trade-offs considered by the organization for managing risk.	10	
			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 systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
PM-29	Risk Management Program Leadership Roles	Risk management program leadership roles should include C-SCRM responsibilities and be included in C-SCRM collaboration across the enterprise. Section 2 and Appendix C provide detailed guidance for C-SCRM roles and responsibilities	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
			Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
PM-30	Supply Chain Risk Management Strategy	The Supply Chain Risk Management Strategy (also known as C-SCRM Strategy) should be complemented with a C-SCRM Implementation Plan that lays out detailed initiatives and activities for the enterprise with timelines and responsible parties. This implementation plan can be a POA&M or be included in a POA&M. Based on the C-SCRM Strategy and Implementation Plan at Level 1, the enterprise should select and document common C- SCRM controls that should address the enterprise, program, and system-specific needs. These controls should be iteratively integrated into the C-SCRM Policy at Level 1 and Level 2, as well as the C-SCRM plan (or SSP if required) at Level 3. See Section 2 and Appendix C for further guidance on risk management.	Functional	Equal	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	10	
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	
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 services or functions to ensure those resources are being used consistent with their intended purpose.	10	
PS-1	Policy and Procedures	At each level, the personnel security policy and procedures and the related C-SCRM Strategy/Implementation Plan, C-SCRM Policies, and C-SCRM Plan(s) need to define the roles for the personnel who are engaged in the acquisition, management, and execution of supply chain security activities. These roles also need to state acquirer personnel responsibilities with regard to relationships with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Policies and procedures need to consider the full system development life cycle of systems and the roles and responsibilities needed to address the various supply chain 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, delivery/receiving, and IT. Roles for the supplier, developer, system integrator, external system service provider, and other ICT/OTrelated service provider personnel responsible for the success of the program should be noted in an agreement between the acquirer and these parties (e.g., contract). The enterprise should require its prime contractors to implement this control and flow down this requirement to	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
			Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
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	
PS-6	Access Agreements	The enterprise should define and document access agreements for all contractors or other external personnel who may need to access the enterprise's data, systems, or network, whether physically or logically. Access agreements should state the appropriate level and method of access to the information system and supply chain network. 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. NOTE: While the audit mechanisms may be implemented in Level 3, the agreement process with required updates	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	
			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	
PS-7	External Personnel Security	Third-party personnel who have access to the enterprise's information systems and networks must meet the same personnel security requirements as enterprise personnel. Examples of such third-party personnel can include the system integrator, developer, supplier, external service provider used for delivery, contractors or service providers who are using the ICT/OT systems, or supplier maintenance personnel brought in to address component technical issues not solvable by the enterprise or system integrator.	Functional	Equal	Third-Party Personnel Security	HRS-10	Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party cybersecurity & data privacy roles and responsibilities.	10	
PT-1	Policy and Procedures	Enterprises should ensure that supply chain concerns are included in PII processing and transparency policies and procedures, as well as the related C-SCRM Strategy/Implementation Plan, C-SCRM Policies, and C-SCRM Plan. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies. 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 requirements. b. Contractors need to abide by relevant laws and policies regarding information (PII and other sensitive information). c. The enterprise should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
			Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data privacy controls.	10	
			Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
RA-1	Policy and Procedures	Risk assessments should be performed at the enterprise, mission/program, and operational levels. The system-level 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 defined.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
			Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
			Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
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 systems and data in accordance with applicable local, state and Federal laws that: ▪ Document the security categorization results (including supporting rationale) in the security plan for systems; and ▪ Ensure the security categorization decision is reviewed and approved by the asset owner.	10	
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 Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	
			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 systems and data.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
RA-5	Vulnerability Monitoring and Scanning	Vulnerability monitoring should cover suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers in the enterprise's supply chain. This includes employing data collection tools to maintain a continuous state of awareness about potential vulnerability to suppliers, as well as the information systems, system components, and raw inputs that they provide through the cybersecurity supply chain. 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 vulnerabilities arise that are not disclosed in the VDR. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
			Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	
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	
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	
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 respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	10	
RA-9	Criticality Analysis	Enterprises should complete a criticality analysis as a prerequisite input to assessments of cybersecurity supply 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 Nation's Cybersecurity.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
			Functional	Intersects With	Criticality Analysis	TDA-06.1	Mechanisms exist to require the developer of the system, system component or service to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5	
			Functional	Intersects With	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
RA-10	Threat Hunting	The C-SCRM threat hunting activities should supplement the enterprise's internal threat hunting activities. As a critical part of the cybersecurity supply chain risk management process, enterprises should actively monitor for 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]).	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	
SA-1	Policy and Procedures	The system and services acquisition policy and procedures should address C-SCRM throughout the acquisition management life cycle process, to include purchases made via charge cards. C-SCRM procurement actions and the resultant contracts should include requirements language or clauses that address which controls are mandatory or desirable and may include implementation specifications, state what is accepted as evidence that the requirement is satisfied, and how conformance to requirements will be verified and validated. C-SCRM should also be included as an evaluation factor. These applicable procurements should not be limited to those that are directly related to providing an ICT/OT product or service. While C-SCRM considerations must be applied to these purchases, C-SCRM should also be 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 evolve continuously through mergers and acquisitions, joint ventures, and other partnership agreements. The policy should help enterprises understand these changes and use the obtained information to inform their C-SCRM activities. Enterprises can obtain the status of such changes through, for example,	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	
			Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
			Functional	Intersects With	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
SA-2	Allocation of Resources	The enterprise should incorporate C-SCRM requirements when determining and establishing the allocation of resources.	Functional	Equal	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects / initiatives.	10	
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.	5	
			Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
SA-4	Acquisition Process	Enterprises are to include C-SCRM requirements, descriptions, and criteria in applicable contractual agreements. 1. Enterprises are to establish baseline and tailorable C-SCRM requirements to apply and incorporate into contractual agreements when procuring a product or service from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. These include but are not limited to: a. C-SCRM requirements that cover regulatory mandates (e.g., the prohibition of certain ICT/OT or suppliers) address identified and selected controls that are applicable to reducing cyber supply chain risk that may be introduced by a procured product or service and that provide assurance that the contractor is sufficiently responsible, capable, and trustworthy. b. Requirements for critical elements in the supply chain to demonstrate the capability to remediate emerging vulnerabilities based on open source information and other sources. c. Requirements for managing intellectual property ownership and responsibilities for elements such as software code; data and information; the manufacturing, development, or integration environment; designs; and proprietary processes when provided to the enterprise for review or use. d. Requirements that address the expected life span of the product or system, any element(s) that may be in a critical path based on their life span, and what is required when end-of-life is near or has been reached. Enterprises should conduct research or solicit information from bidders or existing providers under contract to understand what end-of-life options exist (e.g., replace, upgrade, migrate to a new system, etc.). e. Articulate any circumstances when secondary market components may be permitted. f. Requirements for functional properties, configuration, and implementation information, as well as any 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	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to ensure risk-based technical and functional specifications are established to define a Minimum Viable Product (MVP).	5	
			Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
			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	
			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 information, systems and processes that are in scope by the third-party.	5	
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: ▪ Deliver the system, component, or service with a pre-established, secure configuration implemented; and ▪ Use the pre-established, secure configuration as the default for any subsequent system, component, or service reinstallation or upgrade.	10	
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	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
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 systems, system components or services to produce a plan for the continuous monitoring of cybersecurity & data privacy control effectiveness.	10	
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 systems that describe: ▪ Secure configuration, installation and operation of the system; ▪ Effective use and maintenance of security features/functions; and ▪ Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5	
			Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity & data privacy control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all systems, applications, services and personnel (internal and third-parties).	5	
SA-8	Security and Privacy Engineering Principles	The following security engineering techniques are helpful for managing cybersecurity risks throughout the supply chain. a. Anticipate the maximum possible ways that the ICT/OT product or service can be misused or abused in order to help identify how to protect the product or system from such uses. Address intended and unintended use scenarios in architecture and design. b. Design network and security architectures, systems, and components based on the enterprise's risk tolerance, as 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), and	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
			Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	5	
SA-9	External System Services	C-SCRM supplemental guidance is provided in the control enhancements.	Functional	Equal	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's systems and data.	10	
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 services.	10	
SA-9(3)	External System Services | Establish and Maintain Trust Relationship with Providers	Relationships with providers should meet the following supply chain security requirements: a. The requirements definition is complete and reviewed for accuracy and completeness, including the assignment of criticality to various components and defining operational concepts and associated scenarios for intended and unintended use. b. Requirements are based on needs, relevant compliance drivers, criticality analysis, and assessments of cybersecurity risks throughout the supply chain. 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, system integrators, external system service providers, or other ICT/OT-related service providers' relationship. This is important to know for re-compete, potential change in provider, and to manage system end-of-life processes. h. Establish negotiated agreements for relationship termination to ensure a safe and secure termination, such as removing data from cloud environments. 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	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 systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
			Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
			Functional	Intersects With	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	5	
			Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
			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 cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
			Functional	Intersects With	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data privacy controls.	5	
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	
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	
			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	
			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	
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	
SA-11	Developer Testing and Evaluation	Depending on the origins of components, this control may be implemented differently. For OTS (off-the-shelf) components, the acquirer should conduct research (e.g., via publicly available resources) or request proof to 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	Functional	Equal	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy personnel to: ▪ Create and implement a Security Test and Evaluation (ST&E) plan; ▪ Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and ▪ Document the results of the security testing/evaluation and flaw	10	
SA-15	Development Process, Standards, and Tools	Providing documented and formalized development processes to guide internal and system integrator developers is critical to the enterprise's efforts to effectively mitigate cybersecurity risks throughout the supply chain. The 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	Functional	Equal	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	10	
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	TDA-06.1	Mechanisms exist to require the developer of the system, system component or service to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
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	
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	Functional	Equal	Developer-Provided Training	TDA-16	Mechanisms exist to require the developers of systems, system components or services to provide training on the correct use and operation of the system, system component or service.	10	
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 systems, system components or services to produce a design specification and security architecture that: ▪ 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; ▪ Accurately and completely describes the required security functionality and the allocation of security controls among physical and logical	10	
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	
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 systems, applications and/or services have the requisite skillset and appropriate access authorizations.	10	
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 systems, applications and/or services 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	Acquiring products directly from qualified original equipment manufacturers (OEMs) or their authorized distributors 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 Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Unsupported Systems	TDA-17	Mechanisms exist to prevent unsupported systems by: ▪ Replacing systems when support for the components is no longer available from the developer, vendor or manufacturer; and ▪ Requiring justification and documented approval for the continued use of unsupported system components required to satisfy mission/business needs.	5	
			Functional	Intersects With	Alternate Sources for Continued Support	TDA-17.1	Mechanisms exist to provide in-house support or contract external providers for support with unsupported system components.	5	
SC-1	Policy and Procedures	System and communications protection policies and procedures should address cybersecurity risks throughout the supply chain in relation to the enterprise's processes, systems, and networks. Enterprise-level and program-specific policies help establish and clarify these requirements, and corresponding procedures provide instructions for meeting these requirements. Policies and procedures should include the coordination of communications among and across multiple enterprise entities within the enterprise, as well as the communications methods, external connections, and processes used between the enterprise and its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
	Policy and Procedures		Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
	Policy and Procedures		Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
	Policy and Procedures		Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
SC-4	Information in Shared System Resources	The enterprise may share information system resources with system suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Protecting information in shared resources in support of various supply chain activities is challenging when outsourcing key operations. Enterprises may either share too much and increase their risk or share too little and make it difficult for suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to be efficient in their service delivery. The enterprise should work with developers to define a structure or process for information sharing, including the data shared, the method of sharing, and to whom (the specific roles) the information is provided. Appropriate privacy,	Functional	Equal	Information In Shared Resources	SEA-05	Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.	10	
SC-5	Denial-of-service Protection	C-SCRM Guidance supplemental guidance is provided in control enhancement SC-5 (2).	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of systems that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	
SC-5(2)	Denial-of-service Protection | Capacity, Bandwidth, and Redundancy	The enterprise should include requirements for excess capacity, bandwidth, and redundancy into agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of systems that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	
			Functional	Intersects With	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.	5	
SC-7	Boundary Protection	The enterprise should implement appropriate monitoring mechanisms and processes at the boundaries between the agency systems and suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers' systems. Provisions for boundary protections should be incorporated into agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. There may be multiple interfaces throughout the enterprise, supplier systems and networks, and the SDLC. Appropriate vulnerability, threat, and risk assessments should be performed to ensure proper boundary protections for supply chain components and supply chain information flow. The vulnerability, threat, and risk assessments can aid in	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
SC-7(13)	Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components	The enterprise should provide separation and isolation of development, test, and security assessment tools and operational environments and relevant monitoring tools within the enterprise's information systems and networks. This control applies the entity responsible for creating software and hardware, to include federal agencies and prime contractors. As such, this controls applies to the federal agency and applicable supplier information systems and networks. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. If a compromise or information leakage happens in any one environment, the other environments should still be protected through the separation and isolation mechanisms or techniques.	Functional	Intersects With	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.	5	
SC-7(14)	Boundary Protection | Protect Against Unauthorized Physical Connections	This control is relevant to C-SCRM as it applies to external service providers.	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	
			Functional	Intersects With	Lockable Physical Casings	PES-03.2	Physical access control mechanisms exist to protect system components from unauthorized physical access (e.g., lockable physical casings).	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
			Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
SC-7(19)	Boundary Protection | Block Communication from Non-organizationally Configured Hosts	This control is relevant to C-SCRM as it applies to external service providers.	Functional	Intersects With	Network Access Control (NAC)	AST-02.5	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	5	
SC-8	Transmission Confidentiality and Integrity	The requirements for transmission confidentiality and integrity should be integrated into agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Acquirers, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers may repurpose existing security mechanisms (e.g., authentication, authorization, or encryption) to achieve enterprise confidentiality and integrity requirements. The degree of protection should be based on the sensitivity of information to be transmitted and the relationship between the enterprise and the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier 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	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
			Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
SC-18	Transmission Confidentiality and Integrity	The enterprise should use this control in various applications of mobile code within their information systems and networks. Examples include acquisition processes such as the electronic transmission of supply chain information (e.g., email), the receipt of software components, logistics information management in RFID, or transport sensors infrastructure.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
SC-18(2)	Mobile Code | Acquisition, Development, and Use	The enterprise should employ rigorous supply chain protection techniques in the acquisition, development, and use of mobile code to be deployed in the information system. Examples include ensuring that mobile code originates from vetted sources when acquired, that vetted system integrators are used for the development of custom mobile code or prior to installing, and that verification processes are in place for acceptance criteria prior to installation in order to verify the source and integrity of code. Note that mobile code can be both code for the underlying information systems and networks (e.g., RFID device applications) or for information systems and components.	Functional	Intersects With	Software Licensing Restrictions	AST-02.7	Mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions.	5	
			Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
SC-27	Platform-independent Applications	The use of trusted platform-independent applications is essential to CSCRM. The enhanced portability of platform-independent applications enables enterprises to switch external service providers more readily in the event that one becomes compromised, thereby reducing vendor-dependent cybersecurity risks. This is especially relevant for critical applications on which multiple systems may rely	Functional	Equal	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	10	
SC-28	Protection of Information at Rest	The enterprise should include provisions for the protection of information at rest into their agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The enterprise should also ensure that they provide appropriate protections within the information systems and networks for data at rest for the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers information, such as source code, testing data, blueprints, and intellectual property information. This control should be applied throughout the SDLC, including during requirements, development, manufacturing, test, inventory management, maintenance, and disposal. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
			Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
SC-29	Heterogeneity	Heterogeneity techniques include the use of different operating systems, virtualization techniques, and multiple sources of supply. Multiple sources of supply can improve component availability and reduce the impact of a supply chain cybersecurity compromise. In case of a supply chain cybersecurity compromise, an alternative source of supply will allow the enterprises to more rapidly switch to an alternative system/component that may not be affected by the compromise. Addtionally, heterogeneous components decrease the attack surface by limiting the impact to the subset of the infrastructure that is using vulnerable components.	Functional	Equal	Heterogeneity	SEA-13	Mechanisms exist to utilize a diverse set of technologies for system components to reduce the impact of technical vulnerabilities from the same Original Equipment Manufacturer (OEM).	10	
SC-30	Concealment and Misdirection	Concealment and misdirection techniques for C-SCRM include the establishment of random resupply times, the concealment of location, randomly changing the fake location used, and randomly changing or shifting information storage into alternative servers or storage mechanisms.	Functional	Intersects With	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for systems to confuse and mislead adversaries.	5	
SC-30(2)	Concealment and Misdirection | Randomness	Supply chain processes are necessarily structured with predictable, measurable, and repeatable processes for the purpose of efficiency and cost reduction. This opens up the opportunity for potential breach. In order to protect against compromise, the enterprise should employ techniques to introduce randomness into enterprise operations and assets in the enterprise's systems or networks (e.g., randomly switching among several delivery enterprises or routes, or changing the time and date of receiving supplier software updates if previously predictably scheduled).	Functional	Equal	Randomness	SEA-14.1	Automated mechanisms exist to introduce randomness into organizational operations and assets.	10	
SC-30(3)	Concealment and Misdirection | Change Processing and Storage Locations	Changes in processing or storage locations can be used to protect downloads, deliveries, or associated supply chain metadata. The enterprise may leverage such techniques within the their information systems and networks to create uncertainty about the activities targeted by adversaries. Establishing a few process changes and randomizing their use – whether it is for receiving, acceptance testing, storage, or other supply chain activities – can aid in reducing the likelihood of a supply chain event.	Functional	Equal	Change Processing & Storage Locations	SEA-14.2	Automated mechanisms exist to change the location of processing and/or storage at random time intervals.	10	
SC-30(4)	Concealment and Misdirection | Misleading Information	The enterprise can convey misleading information as part of concealment and misdirection efforts to protect the information system being developed and the enterprise's systems and networks. Examples of such efforts in security include honeynets or virtualized environments. Implementations can be leveraged to convey misleading information. These may be considered advanced techniques that require experienced resources to effectively implement them. If an enterprise decides to use honeypots, it should be done in concert with legal counsel or following the enterprise's policies.	Functional	Intersects With	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for systems to confuse and mislead adversaries.	5	
SC-30(5)	Concealment and Misdirection | Concealment of System Components	The enterprise may employ various concealment and misdirection techniques to protect information about the information system being developed and the enterprise's information systems and networks. For example, the delivery of critical components to a central or trusted third-party depot can be used to conceal or misdirect any information regarding the component's use or the enterprise using the component. Separating components from their associated information into differing physical and electronic delivery channels and obfuscating the information through various techniques can be used to conceal information and reduce the opportunity for a potential loss of confidentiality of the component or its use, condition, or other attributes.	Functional	Intersects With	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for systems to confuse and mislead adversaries.	5	
SC-36	Distributed Processing and Storage	Processing and storage can be distributed both across the enterprise's systems and networks and across the SDLC. The enterprise should ensure that these techniques are applied in both contexts. Development, manufacturing, configuration management, test, maintenance, and operations can use distributed processing and storage. This control applies to the entity responsible for processing and storage functions or related infrastructure, to include federal agencies and contractors. As such, this control applies to the federal agency and applicable supplier information systems and networks. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Equal	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.	10	
SC-37	Out-of-band Channels	C-SCRM-specific supplemental guidance is provided in control enhancement SC-37 (1).	Functional	Intersects With	Out-of-Band Channels	NET-11	Mechanisms exist to utilize out-of-band channels for the electronic transmission of information and/or the physical shipment of system components or devices to authorized individuals.	5	
SC-37(1)	Out-of-band Channels | Ensure Delivery and Transmission	The enterprise should employ security safeguards to ensure that only specific individuals or information systems receive the information about the information system or its development environment and processes. For example, proper credentialing and authorization documents should be requested and verified prior to the release of critical components, such as custom chips, custom software, or information during delivery.	Functional	Intersects With	Out-of-Band Channels	NET-11	Mechanisms exist to utilize out-of-band channels for the electronic transmission of information and/or the physical shipment of system components or devices to authorized individuals.	5	
SC-38	Operations Security	The enterprise should ensure that appropriate supply chain threat and vulnerability information is obtained from and provided to the applicable operational security processes.	Functional	Intersects With	Security Operations Center (SOC)	OPS-04	Mechanisms exist to establish and maintain a Security Operations Center (SOC) that facilitates a 24x7 response capability.	5	
			Functional	Intersects With	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
SC-47	Alternate Communications Channels	If necessary and appropriate, suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers should be included in the alternative communication paths described in this control.	Functional	Equal	Alternate Communications Channels	BCD-10.4	Mechanisms exist to maintain command and control capabilities via alternate communications channels and designating alternative decision makers if primary decision makers are unavailable.	10	
SI-1	Policy and Procedures	The enterprise should include C-SCRM in system and information integrity policy and procedures, including ensuring that program-specific requirements for employing various integrity verification tools and techniques are clearly defined. System and information integrity for information systems, components, and the underlying information systems and networks is critical for managing cybersecurity risks throughout the supply chain. The insertion of malicious code and counterfeits are two primary examples of cybersecurity risks throughout the supply chain, both of which can be at least partially addressed by deploying system and information integrity controls.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
			Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
			Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
SI-2	Flaw Remediation	The output of flaw remediation activities provides useful input into the ICT/OT SCRM processes described in Section 2 and Appendix C. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
			Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	5	
			Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Mechanisms exist to automatically update antimalware technologies, including signature definitions.	5	
SI-2(5)	Flaw Remediation | Automatic Software and Firmware Updates	The enterprise should specify the various software assets within its information systems and networks that require automated updates (both indirect and direct). This specification of assets should be defined from criticality analysis results, which provide information on critical and non-critical functions and components (see Section 2 and Appendix C). A centralized patch management process may be employed for evaluating and managing updates prior to deployment. Those software assets that require direct updates from a supplier should only accept updates that originate directly from the OEM unless specifically deployed by the acquirer, such as with a centralized patch management process. Departments and agencies should refer to Appendix F to implement this guidance in accordance	Functional	Intersects With	Automated Software & Firmware Updates	VPM-05.4	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.	5	
SI-3	Malicious Code Protection	Because the majority of code operated in federal systems is not developed by the Federal Government, malicious code threats often originate from the supply chain. This controls applies to the federal agency and contractors with code-related responsibilities (e.g., developing code, installing patches, performing system upgrades, etc.), as well as applicable contractor information systems and networks. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	5	
			Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
			Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
			Functional	Intersects With	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5	
			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	
			Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Mechanisms exist to automatically update antimalware technologies, including signature definitions.	5	
			Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
SI-4	System Monitoring	This control includes monitoring vulnerabilities that result from past supply chain cybersecurity compromises, such as malicious code implanted during software development and set to activate after deployment. System monitoring is frequently performed by external service providers. Service-level agreements with these providers should be structured to appropriately reflect this control. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
			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	
			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	
			Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
SI-4(17)	System Monitoring | Integrated Situational Awareness	System monitoring information may be correlated with that of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, if appropriate. The results of correlating monitoring information may point to supply chain cybersecurity vulnerabilities that require mitigation or compromises.	Functional	Equal	Integration of Scanning & Other Monitoring Information	MON-02.3	Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity.	10	
SI-4(19)	System Monitoring | Risk for Individuals	Persons identified as being of higher risk may include enterprise employees, contractors, and other third parties (e.g., volunteers, visitors) who may have the need or ability to access to an enterprise's system, network, or system environment. The enterprise may implement enhanced oversight of these higher-risk individuals in accordance with policies, procedures, and – if relevant – terms of an agreement and in coordination with appropriate officials.	Functional	Equal	Individuals Posing Greater Risk	MON-01.14	Mechanisms exist to implement enhanced activity monitoring for individuals who have been identified as posing an increased level of risk.	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
SI-5	Security Alerts, Advisories, and Directives	The enterprise should evaluate security alerts, advisories, and directives for cybersecurity supply chain impacts and follow up if needed. US-CERT, FASC, and other authoritative entities generate security alerts and advisories that are applicable to C-SCRM. Additional laws and regulations will impact who and how additional advisories are provided. Enterprises should ensure that their information-sharing protocols and processes include sharing alerts, advisories, and directives with relevant parties with whom they have an agreement to deliver products or perform services. Enterprises should provide direction or guidance as to what actions are to be taken in response to sharing such an alert, advisory, or directive. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
			Functional	Intersects With	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
			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	
SI-7	Software, Firmware, and Information Integrity	This control applies to the federal agency and applicable supplier products, applications, information systems, and networks. The integrity of all applicable systems and networks should be systematically tested and verified to ensure that it remains as required so that the systems/components traversing through the supply chain are not impacted by unanticipated changes. The integrity of systems and components should also be tested and verified. Applicable verification tools include digital signature or checksum verification; acceptance testing for physical components; confining software to limited privilege environments, such as sandboxes; code execution in contained environments prior to use; and ensuring that if only binary or machine-executable code is available, it is obtained directly from the OEM or a verified supplier or distributer. Mechanisms for this control are discussed in detail in [NIST SP 800-53, Rev. 5]. This control applies to federal agencies and applicable supplier information systems and networks. When purchasing an ICT/OT product, an enterprise should perform due diligence to understand what a supplier's integrity assurance practices are. Enterprises should require their prime contractors to implement this 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	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	5	
			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	
			Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
SI-7(14)	Software, Firmware, and Information Integrity | Binary or Machine Executable Code	The enterprise should obtain binary or machine-executable code directly from the OEM/developer or other verified source.	Functional	Intersects With	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.	5	This control that exists within NIST SP 800-161 R1 was withdrawn from NIST 800-53 R5 and no longer exists.
SI-7(15)	Software, Firmware, and Information Integrity | Code Authentication	The enterprise should ensure that code authentication mechanisms, such as digital signatures, are implemented to ensure the integrity of software, firmware, and information.	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	
SI-12	Information Management and Retention	C-SCRM should be included in information management and retention requirements, especially when the sensitive and proprietary information of a system integrator, supplier, or external service provider is concerned.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
			Functional	Intersects With	Personal Data Retention & Disposal	PRI-05	Mechanisms exist to: ▪ Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; ▪ Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and ▪ Use organization-defined techniques or methods to ensure secure deletion	5	
SI-20	Tainting	Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers may have access to the sensitive information of a federal agency. In this instance, enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Equal	Tainting	THR-08	Mechanisms exist to embed false data or steganographic data in files to enable the organization to determine if data has been exfiltrated and provide a means to identify the individual(s) involved.	10	
SR-1	Policy and Procedures	C-SCRM policies are developed at Level 1 for the overall enterprise and at Level 2 for specific missions and functions. C-SCRM policies can be implemented at Levels 1, 2, and 3, depending on the level of depth and detail. C-SCRM procedures are developed at Level 2 for specific missions and functions and at Level 3 for specific systems. Enterprise functions including but not limited to information security, legal, risk management, and acquisition should review and concur on the development of C-SCRM policies and procedures or provide guidance to system owners for developing system-specific C-SCRM procedures.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
			Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
SR-2	Supply Chain Risk Management Plan	C-SCRM plans describe implementations, requirements, constraints, and implications at the system level. C-SCRM plans are influenced by the enterprise's other risk assessment activities and may inherit and tailor common control baselines defined at Level 1 and Level 2. C-SCRM plans defined at Level 3 work in collaboration with the enterprise's C-SCRM Strategy and Policies (Level 1 and Level 2) and the C-SCRM Implementation Plan (Level 1 and Level 2) to provide a systematic and holistic approach for cybersecurity supply chain risk management across the enterprise. C-SCRM plans should be developed as a standalone document and only integrated into existing system security plans if enterprise constraints require it.	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 systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
			Functional	Intersects With	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	5	
SR-3	Supply Chain Controls and Processes	Section 2 and Appendix C of this document provide detailed guidance on implementing this control. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity.	Functional	Equal	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	10	
SR-3(1)	Supply Chain Controls and Processes | Diverse Supply Base	Enterprises should diversify their supply base, especially for critical ICT/OT products and services. As a part of this exercise, the enterprise should attempt to identify single points of failure and risk among primes and lower-level entities in the supply chain. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis.	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	5	
			Functional	Intersects With	Supplier Diversity	TDA-03.1	Mechanisms exist to obtain cybersecurity & data privacy technologies from different suppliers to minimize supply chain risk.	5	
			Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique systems, system components or services.	5	
SR-3(2)	Supply Chain Controls and Processes | Sub-tier Flow	Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors throughout the SDLC. The use of the acquisition process provides an important vehicle to protect the supply chain. As part of procurement requirements, enterprises should include the need for suppliers to flow down controls to subcontractors throughout the SDLC. As part of market research and analysis activities, enterprises should conduct robust due diligence research on potential suppliers or products, as well as their upstream dependencies (e.g., fourth- and fifth-party suppliers), which can help enterprises avoid single points of failure within	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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 (optional)	Notes (optional)
SR-3(3)	Processes | Sub-tier Flow Down	their supply chains. The results of this research can be helpful in shaping the sourcing approach and refining requirements. An evaluation of the cybersecurity risks that arise from a supplier, product, or service should be completed prior to the contract award decision to ensure that the holistic risk profile is well-understood and serves as a weighted factor in award decisions. During the period of performance, suppliers should be monitored for conformance to the defined controls and requirements, as well as changes in risk conditions. See Section 3 for guidance on the Role of CSCRM in the Acquisition Process	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
SR-4	Provenance	Provenance should be documented for systems, system components, and associated data throughout the SDLC. Enterprises should consider producing SBOMs for applicable and appropriate classes of software, including purchased software, open source software, and in-house software. SBOMs should be produced using only NTIA-supported SBOM formats that can satisfy [NTIA SBOM] EO 14028 NTIA minimum SBOM elements. Enterprises producing SBOMs should use [NTIA SBOM] minimum SBOM elements as framing for the inclusion of primary components. SBOMs should be digitally signed using a verifiable and trusted key. SBOMs can play a critical role in enabling organizations to maintain provenance. However, as SBOMs mature, organizations should ensure they do not deprioritize existing C-SCRM	Functional	Intersects With	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to systems, system components and associated data.	5	
SR-5	Acquisition Strategies, Tools, and Methods	Section 3 and SA controls provide additional guidance on acquisition strategies, tools, and methods. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity.	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique systems, system components or services.	5	
SR-6	Supplier Assessments and Reviews	In general, an enterprise should consider any information pertinent to the security, integrity, resilience, quality, trustworthiness, or authenticity of the supplier or their provided services or products. Enterprises should consider applying this information against a consistent set of core baseline factors and assessment criteria to facilitate equitable comparison (between suppliers and over time). Depending on the specific context and purpose for which the assessment is being conducting, the enterprise may select additional factors. The quality of information (e.g., its relevance, completeness, accuracy, etc.) relied upon for an assessment is also an important consideration. Reference sources for assessment information should also be	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and audit External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	
SR-7	Supply Chain Operations Security	The C-SCRM PMO can help determine OPSEC controls that apply to specific missions and functions. OPSEC controls are particularly important when there is specific concern about an adversarial threat from or to the enterprise's supply chain or an element within the supply chain, or when the nature of the enterprise's mission or business operations, its information, and/or its service/product offerings make it a more attractive target for an adversarial threat.	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 systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
			Functional	Intersects With	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	5	
SR-8	Notification Agreements	At minimum, enterprises should require their suppliers to establish notification agreements with entities within their supply chain that have a role or responsibility related to that critical service or product. 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	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected systems, applications and/or services that the organization utilizes.	10	
SR-9	Tamper Resistance and Detection	Enterprises should apply tamper resistance and detection control to critical components, at a minimum. Criticality analysis can help determine which components are critical. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis. The C-SCRM PMO can help identify critical components, especially those that are used by multiple missions, functions, and systems within an enterprise. 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	Logical Tampering Protection	AST-15	Mechanisms exist to verify logical configuration settings and the physical integrity of critical technology assets throughout their lifecycle.	5	
SR-10	Inspection of Systems or Components	Enterprises should inspect critical systems and components, at a minimum, for assurance that tamper resistance controls are in place and to examine whether there is evidence of tampering. Products or components should be inspected prior to use and periodically thereafter. Inspection requirements should also be included in contracts with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors and flow down to subcontractors, when relevant. Criticality analysis can help determine which systems and components are critical and should therefore be subjected to inspection. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis. The C-SCRM PMO can help identify critical systems and components, especially those that are used by multiple missions, functions, and systems (for components) within an enterprise.	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5	
			Functional	Intersects With	Inspection of Systems, Components & Devices	AST-15.1	Mechanisms exist to physically and logically inspect critical technology assets to detect evidence of tampering.	5	
SR-11	Component Authenticity	The development of anti-counterfeit policies and procedures requires input from and coordination with acquisition, information technology, IT security, legal, and the C-SCRM PMO. The policy and procedures should address regulatory compliance requirements, contract requirements or clauses, and counterfeit reporting processes to enterprises, such as GIDEP and/or other appropriate enterprises. Where applicable and appropriate, the policy should also address the development and use of a qualified bidders list (QBL) and/or qualified manufacturers list (QML). This helps prevent counterfeits through the use of authorized suppliers, wherever possible, and their integration into the organization's supply chain [CISA SCRM WG3]. Departments and agencies should refer to Appendix F to implement this guidance in	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5	
SR-11(1)	Component Authenticity | Anti-counterfeit Training	The C-SCRM PMO can assist in identifying resources that can provide anti-counterfeit training and/or may be able to conduct such training for the enterprise. The CSCRM PMO can also assist in identifying which personnel should receive the training.	Functional	Equal	Anti-Counterfeit Training	TDA-11.1	Mechanisms exist to train personnel to detect counterfeit system components, including hardware, software and firmware.	10	
SR-11(2)	Component Authenticity | Configuration Control for Component Service and Repair	Information technology, IT security, or the C-SCRM PMO should be responsible for establishing and implementing configuration control processes for component service and repair, to include – if applicable – integrating component service and repair into the overall enterprise configuration control processes. Component authenticity should be addressed in contracts when procuring component servicing and repair support.	Functional	Equal	Maintain Configuration Control During Maintenance	MNT-07	Mechanisms exist to maintain proper physical security and configuration control over technology assets awaiting service or repair.	10	
SR-11(3)	Component Authenticity | Anti-counterfeit Scanning	Enterprises should conduct anti-counterfeit scanning for critical components, at a minimum. Criticality analysis can help determine which components are critical and should be subjected to this scanning. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis. The C-SCRM PMO can help identify critical components, especially those used by multiple missions, functions, and systems within an enterprise.	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5	
SR-12	Component Disposal	IT security – in coordination with the C-SCRM PMO – can help establish appropriate component disposal policies, procedures, mechanisms, and techniques.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
			Functional	Intersects With	Component Disposal	TDA-11.2	[deprecated - incorporated into AST-09] Mechanisms exist to dispose of system components using organization-defined techniques and methods to prevent such components from entering the gray market.	5	
SR-13	Supplier Inventory	a. Develop, document, and maintain an inventory of suppliers that: 1. Accurately and minimally reflects the organization's tier one suppliers that may present a cybersecurity risk in the supply chain [Assignment: organization-defined parameters for determining tier one supply chain]; 2. Is at the level of granularity deemed necessary for assessing criticality and supply chain risk, tracking, and reporting; 3. Documents the following information for each tier one supplier (e.g., prime contractor): review and update supplier inventory [Assignment: enterprise-defined frequency]. i. Unique identify for procurement instrument (i.e., contract, task, or delivery order);	Functional	Subset Of	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.	10	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)