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

Focal Document: **NIST SP 800-161 R1 UPD1 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations**
Focal Document URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-161-r1-cscrm.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description NIST SP 800-161 R1 Supplemental C-SCRM Guidance	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
AC-1	Policy and Procedures	Enterprises should specify and include in agreements (e.g., contracting language) access control policies for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers that have access control policies. These should include both physical and logical access to the supply chain and the information system. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtier contractors.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AC-1	Policy and Procedures	Enterprises should specify and include in agreements (e.g., contracting language) access control policies for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers that have access control policies. These should include both physical and logical access to the supply chain and the information system. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtier contractors.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AC-1	Policy and Procedures	Enterprises should specify and include in agreements (e.g., contracting language) access control policies for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers that have access control policies. These should include both physical and logical access to the supply chain and the information system. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtier contractors.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AC-2	Account Management	choose to define a set of roles and associate a level of authorization to ensure proper implementation. Enterprises must ensure that accounts for contractor personnel do not exceed the period of performance of the contract. Privileged accounts should only be established for appropriately vetted contractor personnel. Enterprises should also have processes in place to establish and manage temporary or emergency accounts for contractor personnel that require access to a mission-critical or mission-enabling system during a continuity or emergency event. For example, during a pandemic event, existing contractor personnel who are not able to work due to illness may need to be temporarily backfilled by new contractor staff. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies	Functional	Intersects With	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify:
AC-2	Account Management	Choose to define a set of roles and associate a level of authorization to ensure proper implementation. Enterprises must ensure that accounts for contractor personnel do not exceed the period of performance of the contract. Privileged accounts should only be established for appropriately vetted contractor personnel. Enterprises should also have processes in place to establish and manage temporary or emergency accounts for contractor personnel that require access to a mission-critical or mission-enabling system during a continuity or emergency event. For example, during a pandemic event, existing contractor personnel who are not able to work due to illness may need to be temporarily backfilled by new contractor staff. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify:
AC-2	Account Management	Choose to define a set of roles and associate a level of authorization to ensure proper implementation. Enterprises must ensure that accounts for contractor personnel do not exceed the period of performance of the contract. Privileged accounts should only be established for appropriately vetted contractor personnel. Enterprises should also have processes in place to establish and manage temporary or emergency accounts for contractor personnel that require access to a mission-critical or mission-enabling system during a continuity or emergency event. For example, during a pandemic event, existing contractor personnel who are not able to work due to illness may need to be temporarily backfilled by new contractor staff. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify:
AC-2	Account Management	choose to define a set of roles and associate a level of authorization to ensure proper implementation. Enterprises must ensure that accounts for contractor personnel do not exceed the period of performance of the contract. Privileged accounts should only be established for appropriately vetted contractor personnel. Enterprises should also have processes in place to establish and manage temporary or emergency accounts for contractor personnel that require access to a mission-critical or mission-enabling system during a continuity or emergency event. For example, during a pandemic event, existing contractor personnel who are not able to work due to illness may need to be temporarily backfilled by new contractor staff. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify:
AC-3	Access Enforcement	Ensure that the information systems and the supply chain have appropriate access enforcement mechanisms in place. This includes both physical and logical access enforcement mechanisms, which likely work in coordination for supply chain needs. Enterprises should ensure that a defined consequence framework is in place to address access control violations. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
AC-3	Access Enforcement	Ensure that the information systems and the supply chain have appropriate access enforcement mechanisms in place. This includes both physical and logical access enforcement mechanisms, which likely work in coordination for supply chain needs. Enterprises should ensure that a defined consequence framework is in place to address access control violations. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
AC-3	Access Enforcement	Ensure that the information systems and the supply chain have appropriate access enforcement mechanisms in place. This includes both physical and logical access enforcement mechanisms, which likely work in coordination for supply chain needs. Enterprises should ensure that a defined consequence framework is in place to address access control violations. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
AC-17	Remote Access	or the operation of information systems, enterprises should implement secure remote access mechanisms and allow remote access only to vetted personnel. Remote access to an enterprise's supply chain (including distributed software development environments) should be limited to the enterprise or contractor personnel and only if and as required to perform their tasks. Remote access requirements – such using a secure VPN, employing multi-factor authentication, or limiting access to specified business hours or from specified geographic locations – must be properly defined in agreements. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize each type of remote access to the system prior to allowing such connections.
AC-18	Wireless Access	An enterprise's supply chain may include wireless infrastructure that supports supply chain logistics (e.g., radio-frequency identification device [RFID] support, software call home features). Supply chain systems/components traverse the supply chain as they are moved from one location to another, whether within the enterprise's own environment or during delivery from system integrators or suppliers. Ensuring that appropriate and secure access mechanisms are in place within this supply chain enables the protection of the information systems and components, as well as logistics technologies and metadata used during shipping (e.g., within tracking sensors). The enterprise should explicitly define appropriate wireless access control mechanisms for the supply chain in policy and implement appropriate mechanisms.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and b. Authorize each type of wireless access to the system prior to allowing such connections.
AC-18	Wireless Access	An enterprise's supply chain may include wireless infrastructure that supports supply chain logistics (e.g., radio-frequency identification device [RFID] support, software call home features). Supply chain systems/components traverse the supply chain as they are moved from one location to another, whether within the enterprise's own environment or during delivery from system integrators or suppliers. Ensuring that appropriate and secure access mechanisms are in place within this supply chain enables the protection of the information systems and components, as well as logistics technologies and metadata used during shipping (e.g., within tracking sensors). The enterprise should explicitly define appropriate wireless access control mechanisms for the supply chain in policy and implement appropriate mechanisms.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and b. Authorize each type of wireless access to the system prior to allowing such connections.
AC-19	Access Control for Mobile Devices	The use of mobile devices (e.g., laptops, tablets, e-readers, smartphones, smartwatches) has become common in the supply chain. They are used in direct support of an enterprise's operations, as well as tracking, supply chain logistics, data as information systems, and components that traverse enterprise or systems integrator supply chains. Ensure that access control mechanisms are clearly defined and implemented where relevant when managing enterprise supply chain components. An example of such an implementation includes access control mechanisms implemented for use with remote handheld units in RFID for tracking components that traverse the supply chain. Access control mechanisms should also be implemented on any associated data and metadata tied to the devices.	Functional	Equal	Access Control For Mobile Devices	MDM-02	Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	10	a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and b. Authorize the connection of mobile devices to organizational systems.
AC-20	Use of External Systems	Enterprises' external information systems include those of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Unlike in an acquirer's internal enterprise where direct and continuous monitoring is possible, in the external supplier relationship, information may be shared on an as-needed basis and should be articulated in an agreement. Access to the supply chain from such external information systems should be monitored and audited. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Equal	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	10	a. [Selection (one or more): Establish [Assignment: organization-defined terms and conditions]; Identify [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:
AC-22	Publicly Accessible Content	Within the C-SCRM context, publicly accessible content may include Requests for Information, Requests for Proposal, or information about delivery of systems and components. This information should be reviewed to ensure that only appropriate content is released for public consumption, whether alone or with other information.	Functional	Equal	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	10	a. Designate individuals authorized to make information publicly accessible; b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included;
AT-1	Policy and Procedures	into the security training and awareness policy. C-SCRM training should target both the enterprise and its contractors. The policy should ensure that supply chain cybersecurity role-based training is required for those individuals or functions that touch or impact the supply chain, such as the information system owner, acquisition, supply chain logistics, system engineering, program management, IT, quality, and incident response. C-SCRM training procedures should address: a. Roles throughout the supply chain and system/element life cycle to limit the opportunities and means available to individuals performing these roles that could result in adverse consequences,	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AT-1	Policy and Procedures	into the security training and awareness policy. C-SCRM training should target both the enterprise and its contractors. The policy should ensure that supply chain cybersecurity role-based training is required for those individuals or functions that touch or impact the supply chain, such as the information system owner, acquisition, supply chain logistics, system engineering, program management, IT, quality, and incident response. C-SCRM training procedures should address: a. Roles throughout the supply chain and system/element life cycle to limit the opportunities and means available to individuals performing these roles that could result in adverse consequences,	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AT-1	Policy and Procedures	into the security training and awareness policy. C-SCRM training should target both the enterprise and its contractors. The policy should ensure that supply chain cybersecurity role-based training is required for those individuals or functions that touch or impact the supply chain, such as the information system owner, acquisition, supply chain logistics, system engineering, program management, IT, quality, and incident response. C-SCRM training procedures should address: a. Roles throughout the supply chain and system/element life cycle to limit the opportunities and means available to individuals performing these roles that could result in adverse consequences,	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AT-2(2)	Literacy Training and Awareness | Insider Threat	Enterprises should provide literacy training on recognizing and reporting potential indicators of insider threat within the supply chain. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Equal	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	10	Provide literacy training on recognizing and reporting potential indicators of insider threat.
AT-3	Role-based Training	effectively. Personnel who are part of the acquisition workforce require training on what C-SCRM requirements, clauses, and evaluation factors are necessary to include when conducting procurement and how to incorporate C-SCRM into each acquisition phase. Similar enhanced training requirements should be tailored for personnel responsible for conducting threat assessments. Responding to threats and identified risks requires training in counterintelligence awareness and reporting. Enterprises should ensure that developers receive training on secure development practices as well as the use of vulnerability scanning tools. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028,	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]: b. Before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; and
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	Security, Compliance & Resilience Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including: (1) Initial security, compliance and resilience awareness training; (2) Recurring awareness training; and (3) Technology Assets, Applications and/or Services (TAAS)-specific training.	10	a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and b. Retain individual training records for [Assignment: organization-defined time period].
AU-1	Policy and Procedures	Enterprises must designate a specific official to manage the development, documentation, and dissemination of the audit and accountability policy and procedures to include auditing of the supply chain information systems and network. The audit and accountability policy and procedures should appropriately address tracking activities and their availability for other various supply chain activities, such as configuration management. Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers activities should not be included in such a policy unless those functions are performed within the acquirer's supply chain information systems and network. Audit and accountability policy procedures should appropriately address supplier audits as a way to examine the quality of a particular supplier and the risk they present to the enterprise and the enterprise's	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AU-1	Policy and Procedures	Enterprises must designate a specific official to manage the development, documentation, and dissemination of the audit and accountability policy and procedures to include auditing of the supply chain information systems and network. The audit and accountability policy and procedures should appropriately address tracking activities and their availability for other various supply chain activities, such as configuration management. Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers activities should not be included in such a policy unless those functions are performed within the acquirer's supply chain information systems and network. Audit and accountability policy procedures should appropriately address supplier audits as a way to examine the quality of a particular supplier and the risk they present to the enterprise and the enterprise's	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AU-1	Policy and Procedures	Enterprises must designate a specific official to manage the development, documentation, and dissemination of the audit and accountability policy and procedures to include auditing of the supply chain information systems and network. The audit and accountability policy and procedures should appropriately address tracking activities and their availability for other various supply chain activities, such as configuration management. Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers activities should not be included in such a policy unless those functions are performed within the acquirer's supply chain information systems and network. Audit and accountability policy procedures should appropriately address supplier audits as a way to examine the quality of a particular supplier and the risk they present to the enterprise and the enterprise's	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
AU-2	Event Logging	Software/hardware changes, failed attempts to access supply chain information systems, or the movement of source code. Information on such events should be captured to provide appropriate audit mechanisms and be traceable and verifiable. Information captured may include the type of event, date/time, length, and the frequency of occurrence. Among other things, auditing may help detect misuse of the supply chain information systems or network caused by insider threats. Logs are a key resource when identifying operational trends and long-term problems. As such, enterprises should incorporate reviewing logs at the contract renewal point for vendors to determine whether there is a systemic problem. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
AU-2	Event Logging	Software/hardware changes, failed attempts to access supply chain information systems, or the movement of source code. Information on such events should be captured to provide appropriate audit mechanisms and be traceable and verifiable. Information captured may include the type of event, date/time, length, and the frequency of occurrence. Among other things, auditing may help detect misuse of the supply chain information systems or network caused by insider threats. Logs are a key resource when identifying operational trends and long-term problems. As such, enterprises should incorporate reviewing logs at the contract renewal point for vendors to determine whether there is a systemic problem. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
AU-3	Content of Audit Records	The audit records of a supply chain event should be securely handled and maintained in a manner that conforms to record retention requirements and preserves the integrity of the findings and the confidentiality of the record information and its sources as appropriate. In certain instances, such records may be used in administrative or legal proceedings. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Equal	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and	10	Ensure that audit records contain information that establishes the following: a. What type of event occurred; b. When the event occurred; c. Where the event occurred; d. Source of the event; e. Outcome of the event; and f. Identity of any individuals, subjects, or

FDE #	FDE Name	Focal Document Element (FDE) Description NIST SP 800-161 R1 Supplemental C-SCRM Guidance	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
AU-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 C-SCRM. The enterprise should adjust the level of audit record review based on the risk changes (e.g., active threat intel, risk profile) on a specific vendor. Contracts should explicitly address how audit findings will be reported and adjudicated.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a security incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity; b. Report findings to [Assignment: organization-defined personnel or roles]; and c. Adjust the level of audit record review, analysis,
AU-6	Audit Record Review, Analysis, and Reporting	The enterprise should ensure that both supply chain and information security auditable events are appropriately filtered and correlated for analysis and reporting. For example, if new maintenance or a patch upgrade is recognized to have an invalid digital signature, the identification of the patch arrival qualifies as a supply chain auditable event, while an invalid signature is an information security auditable event. The combination of these two events may provide information valuable to CSCRM. The enterprise should adjust the level of audit record review based on the risk changes (e.g., active threat intel, risk profile) on a specific vendor. Contracts should explicitly address how audit findings will be reported and adjudicated.	Functional	Intersects With	Audit Level Adjustments	MON-02.6	Mechanisms exist to adjust the level of audit review, analysis and reporting based on evolving threat information from law enforcement, industry associations or other credible sources of threat intelligence.	5	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity; b. Report findings to [Assignment: organization-defined personnel or roles]; and c. Adjust the level of audit record review, analysis,
AU-12	Audit Record Generation	Enterprises should ensure that audit record generation mechanisms are in place to capture all relevant supply chain auditable events. Examples of such events include component version updates, component approvals from acceptance testing results, logistics data-capturing inventory, or transportation information. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5	a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and
CA-1	Policy and Procedures	Integrate the development and implementation of assessment and authorization policies and procedures for supply chain cybersecurity into the control assessment and authorization policy and related C-SCRM Strategy/Implementation Plan(s), policies, and system-level plans. To address cybersecurity risks throughout the supply chain, enterprises should develop a C-SCRM policy (or, if required, integrate into existing policies) to direct C-SCRM activities for control assessment and authorization. The C-SCRM policy should define C-SCRM roles and responsibilities within the enterprise for conducting control assessment and authorization, any dependencies among those roles, and the interaction among the roles. Enterprise-wide security and privacy risks should be assessed on an ongoing basis and include supply chain risk assessment results.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that: (a) Addresses purpose, scope, roles, responsibilities
CA-1	Policy and Procedures	Integrate the development and implementation of assessment and authorization policies and procedures for supply chain cybersecurity into the control assessment and authorization policy and related C-SCRM Strategy/Implementation Plan(s), policies, and system-level plans. To address cybersecurity risks throughout the supply chain, enterprises should develop a C-SCRM policy (or, if required, integrate into existing policies) to direct C-SCRM activities for control assessment and authorization. The C-SCRM policy should define C-SCRM roles and responsibilities within the enterprise for conducting control assessment and authorization, any dependencies among those roles, and the interaction among the roles. Enterprise-wide security and privacy risks should be assessed on an ongoing basis and include supply chain risk assessment results.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that: (a) Addresses purpose, scope, roles, responsibilities
CA-1	Policy and Procedures	Integrate the development and implementation of assessment and authorization policies and procedures for supply chain cybersecurity into the control assessment and authorization policy and related C-SCRM Strategy/Implementation Plan(s), policies, and system-level plans. To address cybersecurity risks throughout the supply chain, enterprises should develop a C-SCRM policy (or, if required, integrate into existing policies) to direct C-SCRM activities for control assessment and authorization. The C-SCRM policy should define C-SCRM roles and responsibilities within the enterprise for conducting control assessment and authorization, any dependencies among those roles, and the interaction among the roles. Enterprise-wide security and privacy risks should be assessed on an ongoing basis and include supply chain risk assessment results.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that: (a) Addresses purpose, scope, roles, responsibilities
CA-2	Control Assessments	Ensure that the control assessment plan incorporates relevant C-SCRM controls and control enhancements. The control assessment should cover the assessment of both information systems and the supply chain and ensure that an enterprise-relevant baseline set of controls and control enhancements are identified and used for the assessment. Control assessments can include information from supplier audits, reviews, and supply chain-related information. Enterprises should develop a strategy for collecting information, including a strategy for engaging with providers on supply chain risk assessments. Such collaboration helps enterprises leverage information from providers, reduce redundancy, identify potential courses of action for risk responses, and reduce the burden on providers. CSCRM personnel should review the control assessment.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and
CA-2	Control Assessments	Ensure that the control assessment plan incorporates relevant C-SCRM controls and control enhancements. The control assessment should cover the assessment of both information systems and the supply chain and ensure that an enterprise-relevant baseline set of controls and control enhancements are identified and used for the assessment. Control assessments can include information from supplier audits, reviews, and supply chain-related information. Enterprises should develop a strategy for collecting information, including a strategy for engaging with providers on supply chain risk assessments. Such collaboration helps enterprises leverage information from providers, reduce redundancy, identify potential courses of action for risk responses, and reduce the burden on providers. CSCRM personnel should review the control assessment.	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	5	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and
CA-2	Control Assessments	Ensure that the control assessment plan incorporates relevant C-SCRM controls and control enhancements. The control assessment should cover the assessment of both information systems and the supply chain and ensure that an enterprise-relevant baseline set of controls and control enhancements are identified and used for the assessment. Control assessments can include information from supplier audits, reviews, and supply chain-related information. Enterprises should develop a strategy for collecting information, including a strategy for engaging with providers on supply chain risk assessments. Such collaboration helps enterprises leverage information from providers, reduce redundancy, identify potential courses of action for risk responses, and reduce the burden on providers. CSCRM personnel should review the control assessment.	Functional	Intersects With	Security, Compliance & Resilience in Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and
CA-2	Control Assessments	Ensure that the control assessment plan incorporates relevant C-SCRM controls and control enhancements. The control assessment should cover the assessment of both information systems and the supply chain and ensure that an enterprise-relevant baseline set of controls and control enhancements are identified and used for the assessment. Control assessments can include information from supplier audits, reviews, and supply chain-related information. Enterprises should develop a strategy for collecting information, including a strategy for engaging with providers on supply chain risk assessments. Such collaboration helps enterprises leverage information from providers, reduce redundancy, identify potential courses of action for risk responses, and reduce the burden on providers. CSCRM personnel should review the control assessment.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and
CA-2	Control Assessments	Ensure that the control assessment plan incorporates relevant C-SCRM controls and control enhancements. The control assessment should cover the assessment of both information systems and the supply chain and ensure that an enterprise-relevant baseline set of controls and control enhancements are identified and used for the assessment. Control assessments can include information from supplier audits, reviews, and supply chain-related information. Enterprises should develop a strategy for collecting information, including a strategy for engaging with providers on supply chain risk assessments. Such collaboration helps enterprises leverage information from providers, reduce redundancy, identify potential courses of action for risk responses, and reduce the burden on providers. CSCRM personnel should review the control assessment.	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and
CA-3	Information Exchange	with developers, system integrators, external system service providers, other ICT/OT-related service providers, and – in some cases – suppliers. Proper service-level agreements should be in place to ensure compliance to system information exchange requirements defined by the enterprise, as the transfer of information between systems in different security or privacy domains with different security or privacy policies introduces the risk that such transfers violate one or more domain security or privacy policies. Examples of such interconnections can include: a. A shared development and operational environment between the enterprise and system integrator b. Product update/patch management connection to an off-the-shelf supplier c. Data request and retrieval transactions in a processing system that resides on an external service provider	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.	5	a. Approve and manage the exchange of information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements; [Assignment: organization-defined type of
CA-5	Plan of Action and Milestones	exists for C-SCRM and includes both information systems and the supply chain. The C-SCRM POA&M should include tasks to be accomplished with a recommendation for completion before or after system authorization, the resources required to accomplish the tasks, milestones established to meet the tasks, and the scheduled completion dates for the milestones and tasks. The enterprise should include relevant weaknesses, the impact of weaknesses on information systems or the supply chain, any remediation to address weaknesses, and any continuous monitoring activities in its C-SCRM POA&M. The C-SCRM POA&M should be included as part of the authorization	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection;	5	a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and b. Update existing plan of action and milestones [Assignment: organization-defined frequency] based
CA-6	Authorization	Authorizing officials should include C-SCRM in authorization decisions. To accomplish this, supply chain risks and compensating controls documented in C-SCRM Plans or system security plans and the C-SCRM POA&M should be included in the authorization package as part of the decision-making process. Risks should be determined and associated compensating controls selected based on the output of criticality, threat, and vulnerability analyses. Authorizing officials may use the guidance in Section 2 of this document as well as NISTIR 8179 to guide the assessment process.	Functional	Equal	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	10	a. Assign a senior official as the authorizing official for the system; b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems; c. Ensure that the authorizing official for the system, before commencing operations: 1. Accepts the use of common controls inherited by
CM-1	Policy and Procedures	to the enterprise's ability to establish the provenance of components, including tracking and tracing them through the SDLC and the supply chain. A properly defined and implemented configuration management capability provides greater assurance throughout the SDLC and the supply chain that components are authentic and have not been inappropriately modified. When defining a configuration management policy and procedures, enterprises should address the full SDLC, including procedures for introducing and removing components to and from the enterprise's information system boundary. A configuration management policy should incorporate configuration items, data retention for configuration items and corresponding metadata, and tracking of the configuration item and its metadata. The enterprise should coordinate with suppliers, developers, system integrators, external system	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
CM-1	Policy and Procedures	to the enterprise's ability to establish the provenance of components, including tracking and tracing them through the SDLC and the supply chain. A properly defined and implemented configuration management capability provides greater assurance throughout the SDLC and the supply chain that components are authentic and have not been inappropriately modified. When defining a configuration management policy and procedures, enterprises should address the full SDLC, including procedures for introducing and removing components to and from the enterprise's information system boundary. A configuration management policy should incorporate configuration items, data retention for configuration items and corresponding metadata, and tracking of the configuration item and its metadata. The enterprise should coordinate with suppliers, developers, system integrators, external system	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
CM-1	Policy and Procedures	to the enterprise's ability to establish the provenance of components, including tracking and tracing them through the SDLC and the supply chain. A properly defined and implemented configuration management capability provides greater assurance throughout the SDLC and the supply chain that components are authentic and have not been inappropriately modified. When defining a configuration management policy and procedures, enterprises should address the full SDLC, including procedures for introducing and removing components to and from the enterprise's information system boundary. A configuration management policy should incorporate configuration items, data retention for configuration items and corresponding metadata, and tracking of the configuration item and its metadata. The enterprise should coordinate with suppliers, developers, system integrators, external system	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
CM-2	Baseline Configuration	of the baseline is to provide a starting point for tracking changes to components, code, and/or settings throughout the SDLC. Regular reviews and updates of baseline configurations (i.e., re-baselining) are critical for traceability and provenance. The baseline configuration must take into consideration the enterprise's operational environment and any relevant supplier, developer, system integrator, external system service provider, and other ICT/OT-related service provider involvement with the organization's information systems and networks. If the system integrator, for example, uses the existing organization's infrastructure, appropriate measures should be taken to establish a baseline that reflects an appropriate set of agreed-upon criteria for access and operation. Enterprises should require their prime contractors to implement this control and flow down this requirement to	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5	a. Develop, document, and maintain baseline configuration control, a current baseline configuration of the system; and b. Review and update the baseline configuration of the system: 1. [Assignment: organization-defined frequency]; 2. When required due to [Assignment: organization-defined circumstances]; and
CM-2	Baseline Configuration	of the baseline is to provide a starting point for tracking changes to components, code, and/or settings throughout the SDLC. Regular reviews and updates of baseline configurations (i.e., re-baselining) are critical for traceability and provenance. The baseline configuration must take into consideration the enterprise's operational environment and any relevant supplier, developer, system integrator, external system service provider, and other ICT/OT-related service provider involvement with the organization's information systems and networks. If the system integrator, for example, uses the existing organization's infrastructure, appropriate measures should be taken to establish a baseline that reflects an appropriate set of agreed-upon criteria for access and operation. Enterprises should require their prime contractors to implement this control and flow down this requirement to	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and b. Review and update the baseline configuration of the system: 1. [Assignment: organization-defined frequency]; 2. When required due to [Assignment: organization-defined circumstances]; and
CM-4	Impact Analyses	Enterprises should take changes to the information system and underlying or interoperable systems and networks under consideration to determine whether the impact of these changes affects existing security controls and warrants additional or different protection to maintain an acceptable level of cybersecurity risk throughout the supply chain. Ensure that stakeholders, such as system engineers and system security engineers, are included in the impact analysis activities to provide their perspectives for C-SCRM. NIST SP 800-53, Rev. 5 control enhancement CM-4 (1) is a mechanism that can be used to protect the information system from vulnerabilities that may be introduced through the test environment.	Functional	Equal	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	10	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.
CM-5	Access Restrictions for Change	Enterprises should ensure that requirements regarding physical and logical access restrictions for changes to the information systems and networks are defined and included in the enterprise's implementation of access restrictions. Examples include access restriction for changes to centrally managed processes for software component updates and the deployment of updates or patches.	Functional	Intersects With	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to Technology Assets, Applications and/or Services (TAAS).	5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.
CM-5	Access Restrictions for Change	Enterprises should ensure that requirements regarding physical and logical access restrictions for changes to the information systems and networks are defined and included in the enterprise's implementation of access restrictions. Examples include access restriction for changes to centrally managed processes for software component updates and the deployment of updates or patches.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.
CM-6	Configuration Settings	networks and throughout the SDLC. Methods of oversight include periodic verification, reporting, and review. Resulting information may be shared with various parties that have access to, are connected to, or engage in the creation of the enterprise's information systems and networks on a need-to-know basis. Changes should be tested and approved before they are implemented. Configuration settings should be monitored and audited to alert designated enterprise personnel when a change has occurred. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration settings; c. Identify, document, and approve any deviations
CM-6	Configuration Settings	networks and throughout the SDLC. Methods of oversight include periodic verification, reporting, and review. Resulting information may be shared with various parties that have access to, are connected to, or engage in the creation of the enterprise's information systems and networks on a need-to-know basis. Changes should be tested and approved before they are implemented. Configuration settings should be monitored and audited to alert designated enterprise personnel when a change has occurred. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	5	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration settings; c. Identify, document, and approve any deviations
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 enhancements CM-7 (9) mechanisms can be used to protect information systems and networks from vulnerabilities that may be introduced by the use of unauthorized hardware being connected to enterprise systems. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Equal	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	10	a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services]
CM-8	System Component Inventory	numbers, component owners, and for networked components or devices – machine names and network addresses. Inventory specifications may include the manufacturer, device type, model, serial number, and physical location. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtier contractors. Enterprises should specify the requirements and how information flow is enforced to ensure that only the required information – and no more – is communicated to the various participants in the supply chain. If information is subsetted downstream, there should be information about who created the subset information. Enterprises should consider producing SBOMs for applicable and appropriate classes of software,	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and	5	a. Develop and document an inventory of system components that: 1. Accurately reflects the system; 2. Includes all components within the system; 3. Does not include duplicate accounting of components or components assigned to any other system; 4. Is at the level of granularity deemed necessary
CM-8	System Component Inventory	numbers, component owners, and for networked components or devices – machine names and network addresses. Inventory specifications may include the manufacturer, device type, model, serial number, and physical location. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtier contractors. Enterprises should specify the requirements and how information flow is enforced to ensure that only the required information – and no more – is communicated to the various participants in the supply chain. If information is subsetted downstream, there should be information about who created the subset information. Enterprises should consider producing SBOMs for applicable and appropriate classes of software,	Functional	Intersects With	Component Duplication Avoidance	AST-02.3	Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components that prevents assets from being duplicated in other asset inventories.	5	a. Develop and document an inventory of system components that: 1. Accurately reflects the system; 2. Includes all components within the system; 3. Does not include duplicate accounting of components or components assigned to any other system; 4. Is at the level of granularity deemed necessary
CM-10	Software Usage Restrictions	Enterprises should ensure that licenses for software used within their information systems and networks are documented, tracked, and maintained. Tracking mechanisms should provide for the ability to trace users and the use of licenses to access control information and processes. As an example, when an employee is terminated, a "named user" license should be revoked, and the license documentation should be updated to reflect this change. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Equal	Software Usage Restrictions	CFG-04	Mechanisms exist to enforce software usage restrictions to comply with applicable contract agreements and copyright laws.	10	a. Use software and associated documentation in accordance with contract agreements and copyright laws; b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is

FDE #	FDE Name	Focal Document Element (FDE) Description NIST SP 800-161 R1 Supplemental C-SCRM Guidance	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
CM-11	User-installed Software	This control extends to the enterprise information system and network users who are not employed by the enterprise. These users may be suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Intersects With	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5	a. Establish [Assignment: organization-defined policies] governing the installation of software by users; b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; and c. Monitor policy compliance [Assignment: organization-defined frequency].
CM-11	User-installed Software	This control extends to the enterprise information system and network users who are not employed by the enterprise. These users may be suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Intersects With	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	a. Establish [Assignment: organization-defined policies] governing the installation of software by users; b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; and c. Monitor policy compliance [Assignment: organization-defined frequency].
CP-1	Policy and Procedures	Enterprises should integrate C-SCRM into the contingency planning policy and related SCRM Strategy/Implementation Plan, policies, and SCRM Plan. The policy should cover information systems and the supply chain network and, at a minimum, address scenarios such as: a. Unplanned component failure and subsequent replacement; b. Planned replacement related to feature improvements, maintenance, upgrades, and modernization; and c. Product and/or service disruption.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
CP-1	Policy and Procedures	Enterprises should integrate C-SCRM into the contingency planning policy and related SCRM Strategy/Implementation Plan, policies, and SCRM Plan. The policy should cover information systems and the supply chain network and, at a minimum, address scenarios such as: a. Unplanned component failure and subsequent replacement; b. Planned replacement related to feature improvements, maintenance, upgrades, and modernization; and c. Product and/or service disruption.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
CP-1	Policy and Procedures	Enterprises should integrate C-SCRM into the contingency planning policy and related SCRM Strategy/Implementation Plan, policies, and SCRM Plan. The policy should cover information systems and the supply chain network and, at a minimum, address scenarios such as: a. Unplanned component failure and subsequent replacement; b. Planned replacement related to feature improvements, maintenance, upgrades, and modernization; and c. Product and/or service disruption.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
CP-2	Contingency Plan	Enterprises should define and implement a contingency plan for the supply chain information systems and network to ensure that preparations are in place to mitigate the loss or degradation of data or operations. Contingencies should be put in place for the supply chain, network, information systems (especially critical components), and processes to ensure protection against compromise and provide appropriate failover and timely recovery to an acceptable state of operations.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	a. Develop a contingency plan for the system that: 1. Identifies essential mission and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential mission and
CP-2	Contingency Plan	Enterprises should define and implement a contingency plan for the supply chain information systems and network to ensure that preparations are in place to mitigate the loss or degradation of data or operations. Contingencies should be put in place for the supply chain, network, information systems (especially critical components), and processes to ensure protection against compromise and provide appropriate failover and timely recovery to an acceptable state of operations.	Functional	Intersects With	Ongoing Contingency Planning	BCD-06	Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes); (2) Processes (e.g., new, altered or decommissioned business practices, including third-party services) (3) Technologies (e.g., new, altered or decommissioned technologies); (4) Data (e.g., changes to data flows and/or data repositories); (5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or	5	a. Develop a contingency plan for the system that: 1. Identifies essential mission and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential mission and
CP-3	Contingency Training	Enterprises should ensure that critical suppliers are included in contingency training. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Equal	Contingency Training	BCD-03	Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.	10	a. Provide contingency training to system users consistent with assigned roles and responsibilities: 1. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility; 2. When required by system changes; and 3. [Assignment: organization-defined frequency] thereafter; and
CP-4	Contingency Plan Testing	Enterprises should ensure that critical suppliers are included in contingency testing. The enterprise – in coordination with the service provider(s) – should test continuity/resiliency capabilities, such as failover from a primary production site to a back-up site. This testing may occur separately from a training exercise or be performed during the exercise. Enterprises should reference their C-SCRM threat assessment output to develop scenarios to test how well the enterprise is able to withstand and/or recover from a C-SCRM threat event.	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests]. b. Review the contingency plan test results; and c. Initiate corrective actions, if needed.
CP-4	Contingency Plan Testing	Enterprises should ensure that critical suppliers are included in contingency testing. The enterprise – in coordination with the service provider(s) – should test continuity/resiliency capabilities, such as failover from a primary production site to a back-up site. This testing may occur separately from a training exercise or be performed during the exercise. Enterprises should reference their C-SCRM threat assessment output to develop scenarios to test how well the enterprise is able to withstand and/or recover from a C-SCRM threat event.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests]. b. Review the contingency plan test results; and c. Initiate corrective actions, if needed.
IA-1	Policy and Procedures	The enterprise should – at enterprise-defined intervals – review, enhance, and update their identity and access management policies and procedures to ensure that critical roles and processes within the supply chain network are defined and that the enterprise's critical systems, components, and processes are identified for traceability. This should include the identity of critical components that may not have been considered under identification and authentication in the past. Note that providing identification for all items within the supply chain would be cost-prohibitive, and discretion should be used. The enterprise should update related C-SCRM Strategy/Implementation Plan(s), Policies, and C-SCRM Plans.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IA-1	Policy and Procedures	The enterprise should – at enterprise-defined intervals – review, enhance, and update their identity and access management policies and procedures to ensure that critical roles and processes within the supply chain network are defined and that the enterprise's critical systems, components, and processes are identified for traceability. This should include the identity of critical components that may not have been considered under identification and authentication in the past. Note that providing identification for all items within the supply chain would be cost-prohibitive, and discretion should be used. The enterprise should update related C-SCRM Strategy/Implementation Plan(s), Policies, and C-SCRM Plans.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IA-1	Policy and Procedures	The enterprise should – at enterprise-defined intervals – review, enhance, and update their identity and access management policies and procedures to ensure that critical roles and processes within the supply chain network are defined and that the enterprise's critical systems, components, and processes are identified for traceability. This should include the identity of critical components that may not have been considered under identification and authentication in the past. Note that providing identification for all items within the supply chain would be cost-prohibitive, and discretion should be used. The enterprise should update related C-SCRM Strategy/Implementation Plan(s), Policies, and C-SCRM Plans.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IA-2	Identification and Authentication (organizational Users)	accessing an ICT/OT system or supply chain network. An enterprise user may include employees, individuals deemed to have the equivalent status of employees (e.g., contractors, guest researchers, etc.), and system integrators fulfilling contractor roles. Criteria such as "duration in role" can aid in defining which identification and authentication mechanisms are used. The enterprise may choose to define a set of roles and associate a level of authorization to ensure proper implementation. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's	Functional	Equal	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	10	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.
IA-4	Identifier Management	system's life within the enterprise. For software development, identifiers should be assigned for those components that have achieved configuration item recognition. For devices and operational systems, identifiers should be assigned when the items enter the enterprise's supply chain, such as when they are transferred to the enterprise's ownership or control through shipping and receiving or via download. Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers typically use their own identifiers for tracking purposes within their own supply chain. Enterprises should correlate those identifiers with the enterprise-assigned identifiers for traceability and accountability. Enterprises	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) services, both on-premises and those hosted by an External Service Provider (ESP).	5	Manage system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier; b. Selecting an identifier that identifies an individual, group, role, service, or device; c. Assigning the identifier to the intended individual
IA-4	Identifier Management	system's life within the enterprise. For software development, identifiers should be assigned for those components that have achieved configuration item recognition. For devices and operational systems, identifiers should be assigned when the items enter the enterprise's supply chain, such as when they are transferred to the enterprise's ownership or control through shipping and receiving or via download. Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers typically use their own identifiers for tracking purposes within their own supply chain. Enterprises should correlate those identifiers with the enterprise-assigned identifiers for traceability and accountability. Enterprises	Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	5	Manage system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier; b. Selecting an identifier that identifies an individual, group, role, service, or device; c. Assigning the identifier to the intended individual
IA-5	Authenticator Management	This control facilitates traceability and non-repudiation throughout the supply chain. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	Manage system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; b. Establishing initial authenticator content for any authenticators issued by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
IA-5	Authenticator Management	This control facilitates traceability and non-repudiation throughout the supply chain. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	Manage system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; b. Establishing initial authenticator content for any authenticators issued by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
IA-8	Identification and Authentication (non-organizational Users)	Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers have the potential to engage the enterprise's supply chain for service delivery (e.g., development/integration services, product support, etc.). Enterprises should manage the establishment, auditing, use, and revocation of identification credentials and the authentication of non-enterprise users within the supply chain. Enterprises should also ensure promptness in performing identification and authentication activities, especially in the case of revocation management, to help mitigate exposure to cybersecurity risks throughout the supply chain such as those that arise due to insider threats.	Functional	Equal	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	10	Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.
IR-1	Policy and Procedures	procurements or services which include, or require, the executive agency shall provide the FASC with relevant information concerning the source or covered article, including 1) the supply chain risk information identified through the course of the agency's activities in furtherance of mitigating, identifying, or managing its supply chain risk and 2) the supply chain risk information regarding covered procurement actions by the agency under the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) 41 U.S.C. § 4713; and any orders issued by the agency under 41 U.S.C. § 4713. Bidirectional communication with supply chain partners should be defined in agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IR-1	Policy and Procedures	procurements or services which include, or require, the executive agency shall provide the FASC with relevant information concerning the source or covered article, including 1) the supply chain risk information identified through the course of the agency's activities in furtherance of mitigating, identifying, or managing its supply chain risk and 2) the supply chain risk information regarding covered procurement actions by the agency under the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) 41 U.S.C. § 4713; and any orders issued by the agency under 41 U.S.C. § 4713. Bidirectional communication with supply chain partners should be defined in agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IR-1	Policy and Procedures	procurements or services which include, or require, the executive agency shall provide the FASC with relevant information concerning the source or covered article, including 1) the supply chain risk information identified through the course of the agency's activities in furtherance of mitigating, identifying, or managing its supply chain risk and 2) the supply chain risk information regarding covered procurement actions by the agency under the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) 41 U.S.C. § 4713; and any orders issued by the agency under 41 U.S.C. § 4713. Bidirectional communication with supply chain partners should be defined in agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IR-1	Policy and Procedures	relevant information concerning the source or covered article, including 1) the supply chain risk information identified through the course of the agency's activities in furtherance of mitigating, identifying, or managing its supply chain risk and 2) the supply chain risk information regarding covered procurement actions by the agency under the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) 41 U.S.C. § 4713; and any orders issued by the agency under 41 U.S.C. § 4713. Bidirectional communication with supply chain partners should be defined in agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IR-1	Policy and Procedures	relevant information concerning the source or covered article, including 1) the supply chain risk information identified through the course of the agency's activities in furtherance of mitigating, identifying, or managing its supply chain risk and 2) the supply chain risk information regarding covered procurement actions by the agency under the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) 41 U.S.C. § 4713; and any orders issued by the agency under 41 U.S.C. § 4713. Bidirectional communication with supply chain partners should be defined in agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among
IR-2	Incident Response Training	Enterprises should ensure that critical suppliers are included in incident response training. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	a. Provide incident response training to system users consistent with assigned roles and responsibilities: 1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access; 2. When required by system changes; and 3. [Assignment: organization-defined frequency]
IR-5	Incident Monitoring	Enterprises should ensure that agreements with suppliers include requirements to track and document incidents, response decisions, and activities.	Functional	Equal	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	10	Track and document incidents.