NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2025.3
https://securecontrolsframework.com/set-theory-re

Focal Document:

NIST SP 800-161 R1 Cybersecurity Supply Chain Risk Management Practi
Focal Document URL: https://exc.nist.go/upba/sp/800/161/r1/fatal
Published STRM Lings://exc.enist.go/upba/sp/800/161/r1/fatal
Lings://exc.enist.go/upba/sp/800/161/r1/fatal

FDE#		Focal Document Element (FDE) Description	STRM	STRM			Secure Controls Framework (SCF)	Strength of	
	FDE Name	NIST SP 800-161 R1 Supplemental C-SCRM Guidance	Rationale	Relationship	SCF Control	SCF#	Control Description	Strength of Relationship	Notes (optional)
		Enterprises should specify and include in agreements (e.g., contracting language) access control policies for					Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.		<ul> <li>a. Develop, document, and disseminate to</li> <li>[Assignment: organization-defined personnel or</li> </ul>
		their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related			Publishing Cybersecurity		and data processor position, standards and procedures.		roles]:
AC-1	Policy and Procedures	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	Functional	Intersects With	& Data Protection Documentation	GOV-02		5	<ol> <li>[Selection (one or more): Organization-level;</li> <li>Mission/business process-level; System-level]</li> </ol>
		this control and flow down this requirement to relevant subtier contractors.							access control policy that:
							Mechanisms exist to review the cybersecurity and data protection		(a) Addresses purpose, scope, roles, a. Develop, document, and disseminate to
		Enterprises should specify and include in agreements (e.g., contracting language) access control policies for			Periodic Review &		program, including policies, standards and procedures, at planned		[Assignment: organization-defined personnel or roles]:
AC-1	Policy and Procedures	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	Functional	Intersects With	Update of Cybersecurity	GOV-03	intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	1. [Selection (one or more): Organization-level;
		the supply chain and the information system. Enterprises should require their prime contractors to implement			& Data Protection Program				Mission/business process-level; System-level]
		this control and flow down this requirement to relevant subtier contractors.							access control policy that: (a) Addresses purpose, scope, roles.
		Extermines about a specify and include in agreements (a.g. contrasting language) access control policies for					Mechanisms exist to facilitate the implementation of identification and		a. Develop, document, and disseminate to
		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					access management controls.		[Assignment: organization-defined personnel or roles]:
AC-1	Policy and Procedures	service providers that have access control policies. These should include both physical and logical access to	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01		10	1. [Selection (one or more): Organization-level;
		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.							Mission/business process-level; System-level] access control policy that:
		Use of this control helps establish traceability of actions and actors in the supply chain. This control also							(a) Addresses purpose, scope, roles, a. Define and document the types of accounts
		helps ensure access authorizations of actors in the supply chain is appropriate on a continuous basis. The					Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.		allowed and specifically prohibited for use within
		enterprise may choose to define a set of roles and associate a level of authorization to ensure proper			Termination of	IAC-07.2			the system;
AC-2	Account Management	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	Functional	Intersects With	Employment	IAC-07.2		5	<ul> <li>b. Assign account managers;</li> <li>c. Require [Assignment: organization-defined</li> </ul>
		contractor personnel. Enterprises should also have processes in place to establish and manage temporary or							prerequisites and criteria] for group and role
		emergency accounts for contractor personnel that require access to a mission-critical or mission-enabling.  Use of this control helps establish traceability of actions and actors in the supply chain. This control also					Mechanisms exist to proactively govern account management of		membership: a. Define and document the types of accounts
		helps ensure access authorizations of actors in the supply chain is appropriate on a continuous basis. The enterprise may choose to define a set of roles and associate a level of authorization to ensure proper					individual, group, system, service, application, guest and temporary accounts.		allowed and specifically prohibited for use within the system;
AC-2	Account Management	implementation. Enterprises must ensure that accounts for contractor personnel do not exceed the period of	Functional	Intersects With	Account Management	IAC-15	accounts.	5	b. Assign account managers;
		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							c. Require [Assignment: organization-defined
		emergency accounts for contractor personnel that require access to a mission-critical or mission-enabling							prerequisites and criteria) for group and role membership;
		Use of this control helps establish traceability of actions and actors in the supply chain. This control also helps ensure access authorizations of actors in the supply chain is appropriate on a continuous basis. The					Mechanisms exist to check the validity of information inputs.		<ul> <li>a. Define and document the types of accounts allowed and specifically prohibited for use within</li> </ul>
		enterprise may choose to define a set of roles and associate a level of authorization to ensure proper							the system;
AC-2	Account Management	implementation. Enterprises must ensure that accounts for contractor personnel do not exceed the period of	Functional	Intersects With	Input Data Validation	TDA-18		5	b. Assign account managers;
		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							c. Require [Assignment: organization-defined prerequisites and criteria] for group and role
	1	emergency accounts for contractor personnel that require access to a mission-critical or mission-enabling.  Use of this control helps establish traceability of actions and actors in the supply chain. This control also			1	1	Cryptographic mechanisms exist to implement strong cryptography and		membership: a. Define and document the types of accounts
		helps ensure access authorizations of actors in the supply chain is appropriate on a continuous basis. The			1	1	security protocols to safeguard sensitive/regulated data during		<ul> <li>Define and document the types of accounts</li> <li>allowed and specifically prohibited for use within</li> </ul>
AC-2	Account Management	enterprise may choose to define a set of roles and associate a level of authorization to ensure proper implementation. Enterprises must ensure that accounts for contractor personnel do not exceed the period of	Functional	Intersects With	Safeguarding Data Over	NET-12	transmission over open, public networks.	5	the system; b. Assign account managers;
MO-Z	Account Hanagement	performance of the contract. Privileged accounts should only be established for appropriately vetted	runctional	microeCts with	Open Networks	IVE1-12		٥	c. Require [Assignment: organization-defined
		contractor personnel. Enterprises should also have processes in place to establish and manage temporary or			1	1			prerequisites and criteria] for group and role
		emergency accounts for contractor personnel that require access to a mission-critical or mission-enabling.  Ensure that the information systems and the supply chain have appropriate access enforcement.				1	Mechanisms exist to enforce Logical Access Control (LAC) permissions		membership:
		mechanisms in place. This includes both physical and logical access enforcement mechanisms, which likely					that conform to the principle of "least privilege."		Enforce approved authorizations for logical
AC-3	Access Enforcement	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	Functional	Intersects With	Access Enforcement	IAC-20		5	access to information and system resources in
		to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and							accordance with applicable access control policies.
		agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity.							
		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					Cryptographic mechanisms exist to implement strong cryptography and		
		work in coordination for supply chain needs. Enterprises should ensure that a defined consequence			D. f		security protocols to safeguard sensitive/regulated data during transmission over open, public networks.		Enforce approved authorizations for logical
AC-3	Access Enforcement	framework is in place to address access control violations. Enterprises should require their prime contractors	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12		5	access to information and system resources in accordance with applicable access control
		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,							policies.
		Improving the Nation's Cybersecurity.							
		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					Mechanisms exist to check the validity of information inputs.		L
		work in coordination for supply chain needs. Enterprises should ensure that a defined consequence							Enforce approved authorizations for logical access to information and system resources in
AC-3	Access Enforcement	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	Functional	Intersects With	Input Data Validation	TDA-18		5	accordance with applicable access control
		agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028,							policies.
		Improving the Nation's Cybersecurity.  Prompt revocation is critical to ensure that suppliers, developers, system integrators, external system service					Mechanisms exist to revoke logical and physical access authorizations.		
		providers, and other ICT/OT-related service providers who no longer require access or who abuse or violate							Enforce the revocation of access authorizations
AC-3(8)	Access Enforcement   Revocation of Access	their access privilege are not able to access an enterprise's system. Enterprises should include in their agreements a requirement for contractors and sub-tier contractors to immediately return access credentials	Functional	Equal	Revocation of Access	IAC-20.6		10	resulting from changes to the security attributes
AC-3(8)		agreements a requirement for contractors and sub-tier contractors to immediately return access credentials (e.g., tokens, PfV or CAC cards, etc.) to the enterprise. Enterprises must also have processes in place to	Functional	Equal	Revocation of Access Authorizations	IAC-20.6		10	resulting from changes to the security attributes of subjects and objects based on [Assignment: organization-defined rules governing the timing
AC-3(8)	Revocation of Access	agreements a requirement for contractors and sub-tier contractors to immediately return access credentials (e.g., tokens, PM or CAC cards, etc.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a	Functional	Equal		IAC-20.6		10	resulting from changes to the security attributes of subjects and objects based on [Assignment:
AC-3(8)	Revocation of Access	agreements a requirement for contractors and sub-tier contractors to immediately return access credentials (e.g., tokens, PfV or CAC cards, etc.) to the enterprise. Enterprises must also have processes in place to	Functional	Equal		IAC-20.6	Automated mechanisms exist to validate cybersecurify and data	10	resulting from changes to the security attributes of subjects and objects based on [Assignment: organization-defined rules governing the timing revocations of access authorizations].  Release information outside of the system only it
AC-3(8)	Revocation of Access Authorizations	agreements a requirement for contractors and sub-tier contractors to immediately return access credentials (e.g., tokens, PM, CAC cacis, 4c. 5). One tenterprise. Enteriors must also have processes in place to promptly process the revocation of excess authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrate retempting a nonther with the same personnel supporting. Information about the supply claim should be controlled for release between the enterprise and third parties.	Functional	Equal		IAC-20.6	protection attributes prior to releasing information to external Technology	10	resulting from changes to the security attributes of subjects and objects based on [Assignment: organization-defined rules governing the timing revocations of access authorizations].  Release information outside of the system only (a) The receiving [Assignment: organization-
AC-3(8)	Revocation of Access	agreements a requirement for contractors and sub-lete contractors to immediately return access credentials (e.g., takens, PN occ). Each card, each of the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "budge flipping" situation, a contract is transferred from one system integrator enterprise to another with the same personnel supporting.	Functional	Equal Equal		IAC-20.6 DCH-03.3		10	resulting from changes to the security attributes of subjects and objects based on Assignment: organization-defined rules governing the timing revocations of access authorizations]. Release information outside of the system only (a) The receiving [Assignment: organization-defined system or system component] provided [Assignment: organization-defined system or system component] provided [Assignment: organization-defined controls] and
	Revocation of Access Authorizations  Access Enforcement	speements a requirement for contractors and sub-lete contractors to immediately return access credentials (e.g., takens, PR) or CAC cards, etc.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access suthorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrated enterprise is another with the same personnel supporting information about the supply chain should be controlled for release between the enterprise and third parties information may be exchanged between the enterprise and fits suppliers, developers, system integrators,			Authorizations		protection attributes prior to releasing information to external Technology		resulting from changes to the security attributes of subjects have of no-depicts based on IA-saignment organization-defined rules governing the timing revocations of access authorizations).  Releases information outside of the system only (a) The receiving [Assignment organization-defined system or system component provides [Assignment organization-defined system or system component provides [Assignment organization-defined controls]: and
	Revocation of Access Authorizations  Access Enforcement	speements a requirement for contractors and sub-tier contractors to immediately return access credentials (e.g. tokene, PM CAC Cacid, e.g. to) the enterprise. Enterprise must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract it transferred from one system integrate retempting a norther with the same personnel supporting information about the supply chain should be controlled for release between the enterprise and third parties, information may be exchanged between the enterprise and its suppliers, developers, system integrators, central systems envice providers, and other ICTOT related service providers. The controlled release of enterprise information protects against risks associated with disclosure.			Authorizations		protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).		resulting from changes to the security attributes of subjects and objects based on Assignment: organization-defined rules governing the timing revocations of access authorizations]. Release information outside of the system only (a) The receiving [Assignment: organization-defined system or system component] provided [Assignment: organization-defined system or system component] provided [Assignment: organization-defined controls] and
	Revocation of Access Authorizations  Access Enforcement	speements a requirement for contractors and sub-lete contractors to immediately return access credentials (s.g. Lokene, PRO CAC cards, etc.) to the enterprise. Enterprise must also they processes in piace to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrator enterprise to another with the same personnel supporting information about the supply chain should be controlled for release between the enterprise and third parties. Information may be exchanged between the enterprise and ris suppliers, developers, system integrators, eathernial system service providers, and other ICT/IOT resisted service providers. The controlled release of enterprise information protects against risks associated with disclosure.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the			Authorizations		protection attributes prior to releasing information to external Technology		resulting from changes to the socurity stributes of subjects and objects based on [Assignment-organization-defined rules governing the timing revocations of access subtorizations].  Release information outside of the system only (a) The receiving [Assignment: organization-defined system or system component provider [Assignment: organization-defined system or system component provider [Assignment: organization-defined system or system components organization-defined system or system components or system or syste
AC-3(9)	Revocation of Access Authorizations  Access Enforcement	speements a requirement for contractors and sub-lete contractors to immediately return access credentials (e.g. Lokene, PRO *CAC cards, etc.) to the enterprise. Enterprise must also have processes in piace to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrator enterprise to another with the same personnel supporting information about the supply chain should be controlled for release between the enterprise and third parties, information may be exchanged between the enterprise and fits suppliers, developers, system integrators, external system service providers, and other ICTOT related service providers. The controlled release of enterprise information protects against thick associated with decisiours.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other ICTOT of suppliers, developers, system integrators, external system service providers, and other ICTOT of suppliers, developers, system integrators, external system service providers, and other ICTOT of suppliers, developers, system integrators, external system service providers, and other ICTOT of suppliers, developers, system integrators, external system service providers, and other ICTOT of suppliers, developers, system integrators, external system service providers, and other ICTOT of suppliers, developers, system integrators, external system service providers, and other ICTOT of suppliers, developers, system integrators, external system service providers, and other ICTOT of suppliers, developers, system integrators, external system services providers.	Functional	Equal	Authorizations  Controlled Release  Data Flow Enforcement -	DCH-03.3	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review firewall and router	10	resulting from changes to the security attributes of subjects and objects based on [Assignment: organization-defined rules governing the times proceedings of a cerebing [Assignment: organization-defined rules governing the times (a) The receiving [Assignment: organization-defined system or system component provides [Assignment: organization-defined controls]; and [Assignment: organization-defined controls]; and [Assignment: organization-defined controls]; and [Assignment organization-defined controls]; are used to validate the appropriateness of the information designation of the fact of the controls of the control of the controls of the controls of the controls of the controls of the control of t
	Revocation of Access Authorizations  Access Enforcement   Controlled Release	speements a requirement for contractors and sub-tier contractors to immediately return access credentials (e.g., tokens, PM cOAC cards, etc.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrated restinguishes a motive with the same personnel supporting integrated to the support of the supply chain should be controlled for release between the enterprise and third parties. Information may be exchanged between the enterprise and its suppliers, developers, system integration, sectionally system service providers, and either ICTOT-related service providers. The controlled release of enterprise information protects against risks associated with disclosure.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the emerprise and its survoix federal stakeholders, suppliers, developens, system insignation, service providers, and other ICTOT-related service providers. Specifying the requirements and how information flows is enforced should ensure that only the requirements and how information flows is enforced should ensure that only the requirements and how information flows is enforced should ensure that only the requirement and how information flows in enforced should ensure that only the requirement and how information flows in enforced should ensure that only the requirement and how			Authorizations  Controlled Release		protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review firewall and router configurations to restrict connections between untrusted networks and		resulting from changes to the socurity stribution of usulprest and objects based on [Assignment organization defined rules governing the timing revocations of access authorizations].  Release information outside of the system only (a) The recoking [Assignment organization-defined system or system component provides [Assignment organization-defined system or system component provides [Assignment organization-defined controls]; and [Jassignment organization-defined controls]; and [Jassignment organization-defined controls]; are used to validate the appropriateness of the information designated for releases.
AC-3(9)	Revocation of Access Authorizations  Access Enforcement   Controlled Release	speements a requirement for contractors and sub-tier contractors to immediately return access credentials (e.g., tokene, PM cOAC cards, etc.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrated respirately another with the same personnel supporting integrated to the support of the supply chain should be controlled for release between the enterprise and third parties, information may be exchanged between the enterprise and its suppliers, developers, system integrated systems and the support of the supply chain should be controlled for release between the enterprise and the suppliers, developers, system integration, sectional systems envice providers. The controlled release of enterprise information protects against risks associated with disclosure.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integration, external systems service providers, and other ICTOT -related service providers. Specifying the requirements and how information flow is entroded should ensure that only the requirement for elevant systems service providers, and other ICTOT -related service providers. Specifying the requirements and how information flow is entroded should ensure that only the requirement for elevant and better contractors. Departments and agencies should reform	Functional	Equal	Authorizations  Controlled Release  Data Flow Enforcement – Access Control Lists	DCH-03.3	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review firewall and router configurations to restrict connections between untrusted networks and	10	resulting from changes to the socurity stribution of usulpers and objects based on [Assignment organization defined rules governing the timing revocations of access authorizations].  Release information outside of the system only (a) The receiving [Assignment organization-defined system or system component provides [Assignment organization-defined controls] and [Assignment organization-defined controls] and [Assignment organization-defined controls] are used to validate the appropriateness of the information destinated for releases.  Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on
AC-3(9)	Revocation of Access Authorizations  Access Enforcement   Controlled Release	speements a requirement for contractors and sub-tier contractors to immediately return access credentials (e.g. Lokene, PRO *CAC cards, etc.) to the enterprise. Enterprises must also have processes in piace to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrator enterprise to another with the same personnel supporting information about the supply chain should be controlled for release between the enterprise and third parties, information about the supply chain should be controlled for release between the enterprise and third parties, information may be exchanged between the enterprise and fits suppliers, developers, system integrators, examinal system service providers, and other ICTOT related service providers. The controlled release of enterprise information protects against thick associated with decisiours.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other ICTOT of staked service providers, Specifying the requirements and how information flow is enforced should ensure that only the required information is communicated to various participants in the repulse should ensure that only the required information is communicated to various participants in the repulse control implement this control to implement this control to implement this control to the providers, and the prime contractors to implement this control or control or communicated to various and the providers and the prime contractors to implement this control or control or control or communicated to review the control of the prime contractors to implement this control or control or control or control or control or control or communicated to various developers.	Functional	Equal	Authorizations  Controlled Release  Data Flow Enforcement – Access Control Lists	DCH-03.3	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review firewall and router configurations to restrict connections between unsusted networks and internal systems.	10	resulting from changes to the security attributes or subjects and objects based on [Assignment-organization-defined rules governing the timing revocations of access authorizations].  Release information outside of the system only (a) The receiving [Assignment: organization-defined postem or system component provides (Assignment: organization-defined controls; an (b) [Assignment: organization-defined controls; an object of the control of
AC-3(9)	Revocation of Access Authorizations  Access Enforcement   Controlled Release	speements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM CAC Cacid, etc.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrate enterprise is another with the same personnel supporting into the supply chain should be controlled for release between the enterprise and third parties, information may be exchanged between the enterprise and its suppliers, developers, system integration, external systems envice providers, and other ICTOT-related service providers. The controlled release of enterprise information protects against risks associated with disclosure.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other ICTOT-related service providers. Specifying the requirements and how information those in softrode should ensure that only the required information is communicated to various participants in the supply chain. Enterprises should require their prime contractors to implement this control and for various participants in the supply chain in the information with European and their to Accessital. It is intellement this custom is able to construction with European Specific price 14028, improved refer to Accessital From Intellement this surdinar is a better or the contribution of the following services and includes a section with the SOCCE. For example,	Functional	Equal	Authorizations  Controlled Release  Data Flow Enforcement – Access Control Lists	DCH-03.3	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review firewall and router configurations to trestrict connections between untuated retworks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control	10	resulting from changes to the security attributes or subjects and objects based on [Assignment-organization-defined rules governing the timing revocations of access authorizations].  Release information outside of the system only (a) The receiving [Assignment: organization-defined postem or system component provides (Assignment: organization-defined controls; an (b) [Assignment: organization-defined controls; an object of the control of
AC-3(9)	Revocation of Access Authorizations  Access Enforcement   Controlled Release	speements a requirement for contractors and sub-lete contractors to immediately return access credentials (e.g., tokens, PRO *CAC cards, etc.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrator enterprise and only any processes in place is supported in the same personnel supporting integrators, and the support of the support	Functional	Equal	Authorizations  Controlled Release  Data Flow Enforcement  Access Control Lists (ACLs)	DCH-03.3	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review firewall and router configurations to restrict connections between untrusted networks and internal systems.  Mechanisms exist to associate security attributes with information, source	10	resulting from changes to the security stributes or subjects and objects based on [Assignment- organization-defined rules governing the timing revocation of access authorizations].  Release information notation of the system or particular or access authorizations. In the control of the particular or system component provides (Assignment organization-defined controls); and (I) [Assignment organization-defined controls) and (I) [Assignment organization-defined controls) are used to validate the appropriateness (In the low of information within the system and between connected systems based on [Assignment-organization-defined information flow control policies].
AC-3(9) AC-4	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement	speements a requirement for contractors and sub-lete contractors to immediately return access credentials (e.g., tokens, Pto CAC Cards, etc.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrator enterprise must also have previously integrator of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrator enterprise and its suppliers, developers, system integrators, external systems excipe providers, and other ICTOT related aerice providers. The controlled release of enterprise information may be exchanged between the enterprise and its suppliers, developers, system integrators, external systems excipe providers, and other ICTOT related aerice providers. The controlled release of enterprise information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various florent stakeholders, suppliers, developers, system integrators, external system excive providers, and other ICTOT related enteries providers. Specifying the registration, external system enterprise information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and the ICTOT related aerice providers. Specifying the registration and the ICTOT related aerice providers. Specifying the registration are included as extended as the control and for other than exportment to relevant abuse for control-costs. Specifying the registration are control and flow down this requirement to relevant abuse for control-costs. Departments and agences should relevant to Accendix Et is insolement this quidance in accordance with Executive Order 14028. Insorvioris the Nation's The metadata relevant to CS-CSEOR is extensive and includes activities within the SDLC. For example, information about the control and the ICTOT related in details, and deterprise considered	Functional	Equat Equat	Authorizations  Controlled Release  Data Flow Enforcement - Access Control Lists (ACLs)	DCH-03.3	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review firewall and router configurations to trestrict connections between untuated retworks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control	10	resulting from changes to the socurity attributes or subjects and objects based on [Assignment-organization-defined rules governing the timing revocations of access authorizations].  Release information outside of the system only (a) The receiving [Assignment coganization-defined postem or system component provides [Assignment organization-defined controls]; an object of the component organization-defined controls]; and object of the component organization-defined controls]; are used to validate the appropriations of the momentum of the control of the con
AC-3(9) AC-4	Revocation of Access Authorizations  Access Enforcement   Controlled Release	speements a requirement for contractors and sub-tier contractors to immediately return access credentials (e.g., tokens, PM CAC Cacid, etc.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transfered from one system integrate enterprise is another with the same personnel supporting intomation about the supply chain should be controlled for release between the enterprise and third parties, information may be exchanged between the enterprise and its suppliers, developers, system integration, external systems envice providers, and their (CTOT -related service providers. The controlled release of enterprise information protect against risks associated with disclosure.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its survois federal stakeholders, suppliers, developers, system integrators, external system service providers, and other ICTOT -related providers. Specifying the requirements and how information thous in softward account of the suppliers of the survois suppliers and their control of the survois s	Functional	Equat Equat	Authorizations  Controlled Release  Data Flow Enforcement  Access Control Lists (ACLs)	DCH-03.3	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review firewall and router configurations to trestrict connections between untuated retworks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control	10	resulting from changes to the security stributes or subjects and objects based on [Assignment- organization-defined rules governing the timing revocation of access authorizations].  Release information notation of the system or particular or access authorizations. In the control of the particular or system component provides (Assignment organization-defined controls); and (I) [Assignment organization-defined controls) and (I) [Assignment organization-defined controls) are used to validate the appropriateness (In the low of information within the system and between connected systems based on [Assignment-organization-defined information flow control policies].
AC-3(9) AC-4	Revocation of Access Authorizations  Access Enforcement   Controlled Release	speements a requirement for contractors and sub-lete contractors to immediately return access credentials (e.g., tokens, Pto CAC Cards, etc.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrator enterprise must also have previously integrator of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrator enterprise and its suppliers, developers, system integrators, external systems excipe providers, and other ICTOT related aerice providers. The controlled release of enterprise information may be exchanged between the enterprise and its suppliers, developers, system integrators, external systems excipe providers, and other ICTOT related aerice providers. The controlled release of enterprise information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various florent stakeholders, suppliers, developers, system integrators, external system excive providers, and other ICTOT related enteries providers. Specifying the registration, external system enterprise information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and the ICTOT related aerice providers. Specifying the registration and the ICTOT related aerice providers. Specifying the registration are included as extended as the control and for other than exportment to relevant abuse for control-costs. Specifying the registration are control and flow down this requirement to relevant abuse for control-costs. Departments and agences should relevant to Accendix Et is insolement this quidance in accordance with Executive Order 14028. Insorvioris the Nation's The metadata relevant to CS-CSEOR is extensive and includes activities within the SDLC. For example, information about the control and the ICTOT related in details, and deterprise considered	Functional	Equat Equat	Authorizations  Controlled Release  Data Flow Enforcement  Access Control Lists (ACLs)	DCH-03.3	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review firewall and router configurations to restrict connections between untrusted networks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source	10	resulting from changes to the society attributes or subjects and objects based on [Assignment-organization-defined rules governing the timing revocations of access authorizations].  Release information outside of the system only (s) The receiving [Assignment caganization-defined postern or system componently provides [Assignment organization-defined controls; and by [Assignment organization-defined controls; and by [Assignment organization-defined controls; and by [Assignment organization-defined system and between connected systems based on [Assignment organization defined information flow control based on [Assignment organization-defined information flow control based on [Assignment organization-defined metadata].
AC-3(9) AC-4	Revocation of Access Authorizations  Access Enforcement   Controlled Release	speements a requirement for contractors and sub-lete contractors to immediately return access credentials (e.g., tokens, Pto CAC Cards, etc.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrator enterprise must also have previously integrator of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrator enterprise and its suppliers, developers, system integrators, external systems excipe providers, and other ICTOT related aerice providers. The controlled release of enterprise information may be exchanged between the enterprise and its suppliers, developers, system integrators, external systems excipe providers, and other ICTOT related aerice providers. The controlled release of enterprise information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various florent stakeholders, suppliers, developers, system integrators, external system excive providers, and other ICTOT related enteries providers. Specifying the registration, external system enterprise information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and the ICTOT related aerice providers. Specifying the registration and the ICTOT related aerice providers. Specifying the registration are included as extended as the control and for other than exportment to relevant abuse for control-costs. Specifying the registration are control and flow down this requirement to relevant abuse for control-costs. Departments and agences should relevant to Accendix Et is insolement this quidance in accordance with Executive Order 14028. Insorvioris the Nation's The metadata relevant to CS-CSEOR is extensive and includes activities within the SDLC. For example, information about the control and the ICTOT related in details, and deterprise considered	Functional	Equat Equat	Authorizations  Controlled Release  Data Flow Enforcement— Access Control Lists (ACLs)  Object Security Attributes	DCH-03.3	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Nechanisms exist to design, implement and review frewall and router configurations to restrict connections between untrusted retworks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enflore defined information flow control configurations as a basis for flow control decisions.	10	resulting from changes to the society attributes or subjects and objects based on [Assignment-organization-defined rules governing the timing revocations of access subtrotrations].  Release information outside of the system only (a) The receiving [Assignment organization-defined system or system component provides defined system or system component provides of the system or
AC-3(9) AC-4	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata	speements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM or CAC cards, 4c.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract it transferred from one system integrate enterprise is another with the same personnel supporting into the supply chain should be controlled for release between the enterprise and third parties, information may be exchanged between the enterprise and its suppliers, developers, system integration, external systems envice providers, and other it (TOT -related service providers. The controlled release of enterprise information protects against risks associated with disclosure.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and it various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other iCTOT-related providers. Specifying the requirements and how information those is entroded should ensure that only the required information is communicated to various participants in the supply chain. Enterprises should require their prime contractors to implement this control information that is enterprised and interest and between the prime contractors to implement this control can define the control of the co	Functional	Equat Equat	Authorizations  Controlled Release  Data Flow Enforcement Access Control Lists (ACLs)  Object Security Attributes  Cross Domain	DCH-03.3	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review firewall and router configurations to restrict connections between untrusted networks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source	10	resulting from changes to the security stribution or ubujects and objects based on [Assignment- organization-defined rules governing the timing revocation of access authorizations].  Release information outside of the system conjugation of the partner organization-defined outside of the system or system component provides and system or system component provides are used to validate the appropriateness of the information defined controlls and bij Assignment organization-defined controlls are used to validate the appropriateness are used to validate the appropriateness of the information designated for presence.  Enforce approved systems based on [Assignment- organization-defined information flow control patients].  Enforce information flow control based on [Assignment- organization-defined information flow control policies].  Uniquely identify and authenticate source and designation for promoting by [Selection (nor morno)].
AC-3(9)  AC-4  AC-4(1)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Information Flow Enforcement   Metadata	speements a requirement for contractors and sub-tier contractors to immediately return access credentials (e.g., tokens, PM cOAC cards, etc.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrated respirate a unother with the same personnel supporting integrated to the support of the supply chain should be controlled for release between the enterprise and third parties, information may be exchanged between the enterprise and its suppliers, developers, system integrated sections of the supply chain in the supply chain in the supply chain to a broad set of stakeholders. The controlled release of enterprise information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other ICTOT-related providers. Specifying the requirements and how information flow is entroced should ensure that only the required information is communicated to various participants in the supply chain. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant abulled requirement to execute abulled resolution of the supply chain to a Section of the supply chain in the supply chain to a supply chain to a broad set of stakeholders, including the enterprise and other than the control of the supply chain information flow of the supply chain to a supply chain information flow of the supply chain informat	Functional  Functional	Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement— Access Control Lists (ACLs)  Object Security Attributes	DCH-03.3  NET-04  NET-04.2	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review firewall and router configurations to restrict connections between untrusted networks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source	10	resulting from changes to the society attributes or subjects and objects based on [Assignment-organization-defined rules governing the timing revocations of access subtrotrations].  Release information outside of the system only (a) The receiving [Assignment organization-defined system or system component provides defined system or system component provides of the system or
AC-3(9)  AC-4  AC-4(1)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata	speements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM or CAC cards, 4c.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract it transferred from one system integrate enterprise is another with the same personnel supporting into the supply chain should be controlled for release between the enterprise and third parties, information may be exchanged between the enterprise and its suppliers, developers, system integration, external systems envice providers, and other it (TOT -related service providers. The controlled release of enterprise information protects against risks associated with disclosure.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and it various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other iCTOT-related providers. Specifying the requirements and how information those is entroded should ensure that only the required information is communicated to various participants in the supply chain. Enterprises should require their prime contractors to implement this control information that is enterprised and interest and between the prime contractors to implement this control can define the control of the co	Functional  Functional	Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement Access Control Lists (ACLs)  Object Security Attributes  Cross Domain	DCH-03.3  NET-04  NET-04.2	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and couter configurations to restrict connections between untrusted networks and intermal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.	10	resulting from changes to the society attributes or subjects and objects based on [Assignment-organization-defined rules governing the timing revocations of access subnotizations].  Release information outside of the system only (a) The receiving [Assignment organization-defined system or system componently provides defined system or system componently provides of the system or
AC-3(9)  AC-4  AC-4(1)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata	speements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM or CAC cards, 4c., 10) the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract it transferred from one system integrate enterprise is a notifier with the same personnel supporting intomation about the supply chain should be controlled for release between the enterprise and the supplication may be exchanged between the enterprise and its suppliers, developers, system integration, external system service providers, and other it (TOT -related service providers. The controlled release of enterprise information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other it (TOT -related service providers, and other it (TOT -related service providers, specifying the requirements and how information those is entroded should ensure that only the requirement traverse and the service providers, and other it (TOT -related service providers, Specifying the requirements and how information those is entroded should ensure that only the requirement and the service providers and service providers. Application of the service service service is the service service service service services and the service services are serviced services. The service services are serviced services and service services services and services are of the services	Functional  Functional	Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement Access Control Lists (ACLs)  Object Security Attributes  Cross Domain	DCH-03.3  NET-04  NET-04.2	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review firewall and router configurations to treatrict connections between untrusted retworks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.	10	resulting from changes to the society attributes or subjects and objects based on [Assignment-organization-defined rules governing the timing revocations of access authorizations].  Release information outside of the system only (a) The receiving [Assignment organization-defined postern or system componently provides [Assignment organization-defined controls; an object of the control of the co
AC-3(9)  AC-4  AC-4(17)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata Information Flow Enforcement   Metadata Information Flow Enforcement   Demain Authentication Information Flow	speements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM or CAC cards, 4c.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract it transferred from one system integrate enterprise is another with the same personnel supporting into the supply chain should be controlled for release between the enterprise and third parties, information may be exchanged between the enterprise and its suppliers, developers, system integration, external systems envice providers, and other it (TOT -related service providers. The controlled release of enterprise information protects against risks associated with disclosure.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and it various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other iCTOT-related providers. Specifying the requirements and how information those is entroded should ensure that only the required information is communicated to various participants in the supply chain. Enterprises should require their prime contractors to implement this control information that is enterprised and interest and between the prime contractors to implement this control can define the control of the co	Functional  Functional  Functional	Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement - Access Control Lists (ACLs)  Object Security - Attributes  Cross Domain - Authentication	DCH-03.3  NET-04  NET-04.2	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and couter configurations to restrict connections between untrusted networks and intermal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.	10	resulting from changes to the society attributes or subjects and objects based on [Assignment-organization-defined rules governing the timing revocations of access subnotizations].  Release information outside of the system only (a) The receiving [Assignment organization-defined system or system componently provides defined system or system componently provides of the system or
AC-3(9)  AC-4  AC-4(1)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata	specements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., takens, PM CAC Cacid, s.et, 10 to the enterprise. Enterprise must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transfered from one system integrator enterprise as a notifice with the support of the supply chain should be controlled for release between the enterprise and third parties. Information nabout the supply chain should be controlled for release between the enterprise and third parties. Information may be exchanged between the enterprise and its suppliers, developers, system integrators, external system service providers. In other ICTOI -related service providers. In other Integrators, settlem states of enterprise and its various feetent takes associated with disclosure.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various feetent stakeholders, suppliers, developers, system integrators, external system enterprises and the various feeting that the state of the stakeholders, including the enterprise and includes are integrated in the stakeholders, including the enterprise and the stakeholders are supplicated to various participants in the supply chain. The related state of the stakeholders are included as a stakeholders, including the enterprise and the stakeholders. Including the enterprise and specific soft of the stakeholders included to various and flow down this requirement to relevant sub-lete contractors. Departments and agencies should relate the armount of the stakeholders are supply chain and participants in the accordance with Executive Order 13022, Immediate the Nation's and Committee and th	Functional  Functional	Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement Access Control Lists (ACLs)  Object Security Attributes  Cross Domain	DCH-03.3  NET-04  NET-04.2	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review firewall and router configurations to treatrict connections between untrusted retworks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.	10	resulting from changes to the society attributes or subjects and objects based on [Assignment-organization-defined rules governing the timing revocations of access subnotrations].  Release information outside of the system only (a) The resching [Assignment organization-defined controls] and access of the system only (a) The resching [Assignment organization-defined controls] and but [Assignment organization-defined controls] and but [Assignment organization-defined information flow control patients of the controls of the control
AC-3(9)  AC-4  AC-4(17)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata Information Flow Enforcement   Metadata Information Flow Enforcement   Demain Authentication Information Flow	speements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM CAC Cards, 4c, 61) of the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract its transferd from one system integrate enterprise is another with the same personnel supporting intomation about the supply chain should be controlled for release between the enterprise and third parties, information may be exchanged between the enterprise and its suppliers, developers, system integration, external systems envice providers, and their (CTOT-related exercise providers. The controlled release of enterprise information protect against risks associated with disclosure.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other ICTOT-related providers. Specifying the requirements and how information those is entroded should ensure that only the required information is communicated to various participants in the supply chain. Enterprises should require their prime contractors to implement this control and flow down that requirement to relevant as the decorations. Departments and agencies should refer to Accessful F to intellement this suitance in accordance with Execution Order 16038. Immonitor this Notice and may require approprise protections. Enterprises and besides activities with the SCD. For example, information about systems and system components, acquisition details, and delivery is considered metadata and may require approprise protections. Enterprises should defer to their supply chain security and ensure that information flow enforcement is implemented in order to protect applicable metadata.  For C-SCRM, the validation of data and the relationship to its metadata are critical. Much of the	Functional  Functional  Functional	Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement - Access Control Lists (ACLs)  Object Security - Attributes  Cross Domain - Authentication	DCH-03.3  NET-04  NET-04.2	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review firewall and router configurations to treatrict connections between untrusted retworks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.	10	resulting from changes to the security attributes or subjects and objects based on [Assignment- organization-defined rules governing the timing revocation of access authorizations].  Release information outside of the system conjugation of the program of the pr
AC-3(9)  AC-4  AC-4(1)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata	specements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., takens, PM CAC Cacid, s.et, 10 to the enterprise. Enterprise must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transfered from one system integrator enterprise as a notifice with the support of the supply chain should be controlled for release between the enterprise and third parties. Information nabout the supply chain should be controlled for release between the enterprise and third parties. Information may be exchanged between the enterprise and its suppliers, developers, system integrators, external system service providers. In other ICTOI -related service providers. In other Integrators, settlem states of enterprise and its various feetent takes associated with disclosure.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various feetent stakeholders, suppliers, developers, system integrators, external system enterprises and the various feeting that the state of the stakeholders, including the enterprise and includes are integrated in the stakeholders, including the enterprise and the stakeholders are supplicated to various participants in the supply chain. The related state of the stakeholders are included as a stakeholders, including the enterprise and the stakeholders. Including the enterprise and specific soft of the stakeholders included to various and flow down this requirement to relevant sub-lete contractors. Departments and agencies should relate the armount of the stakeholders are supply chain and participants in the accordance with Executive Order 13022, Immediate the Nation's and Committee and th	Functional  Functional  Functional	Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement - Access Control Lists (ACLs)  Object Security - Attributes  Cross Domain - Authentication	DCH-03.3  NET-04  NET-04.2	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and router configurations to restrict connections between untrusted networks and intermal systems.  Pachanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to apply cybersecurity and/or data protection filters on metadata.	10	resulting from changes to the society attributes or subjects and objects based on [Assignment-organization-defined rules governing the timing revocations of access subnotrations].  Release information outside of the system only (a) The resching [Assignment organization-defined controls] and access of the system only (a) The resching [Assignment organization-defined controls] and but [Assignment organization-defined controls] and but [Assignment organization-defined information flow control patients of the controls of the control
AC-4(17)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata	specements a requirement for contractors and sub-tier contractors to immediately return access credentials (e.g., Lokens, PRO CAC Cacid, s.et.) of the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transfered from one system integrator enterprise a not not way that the contract is transfered from one system integrator enterprise as not not way. The contract is transfered from one system integrator enterprise and its suppliers, developers, system integrators, settlem system service providers. In other with the same personnel supporting, and settlem system service providers and settlem service providers. In developers, system integrators, external system service providers and external postume service providers. In developers, system integrators, external system service providers and external system service providers. Set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integrators, external system service providers. Set of stakeholders, including the enterprise and the various federal stakeholders, suppliers, developers, system integrators, external system service providers. Set of stakeholders, including the enterprise information may traverse a large supply chain to a broad set of stakeholders, including the enterprise information in systems service providers. Set of stakeholders, including the enterprise information in systems service providers. Specifying the requirement system service providers, and other large supply chains to a broad set of stakeholders, including the enterprise should repet to a providers. Specifying the requirement state outland services and flow down this requirement to relevant sub-ter contractors. Specifying the requirement this control and flow down this requirement to relevant sub-ter contractors. Departments and agencies should repet to should repet to should repet to imprise a flow of the st	Functional  Functional  Functional	Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement - Access Control Lists (ACLs)  Object Security - Attributes  Cross Domain - Authentication	DCH-03.3  NET-04  NET-04.2	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and couter configurations to restrict connections between untrusted networks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely objects of the properties	10	resulting from changes to the security stribution or subjects and objects based on [Assignment-organization-defined rules governing the timing revocations of access subnorizations].  Release information outside of the system only (a) The receiving [Assignment organization-defined system or system component [10] (a) The receiving [Assignment organization-defined options or system component [10] (a) the receiving [Assignment organization-defined controls) are used to validate the appropriateness the appropriateness are used to validate the appropriateness are used to validate the appropriateness and between connected systems based on [Assignment organization-defined information flow control based on [Assignment organization-defined metadata].  Enforce information flow control based on [Assignment organization-defined metadata].  Uniquely identify and authenticate source and destination points by [Selection (nee or more): organization-defined metadata].  When transferring information between different security domains, implement [Assignment. organization-defined metadata].  When transferring information between different security domains, implement [Assignment. organization-defined security or privacy policy filters] on metadata.
AC-4(1)  AC-4(17)  AC-4(19)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata	speements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM CAC Cards, etc.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract its transferd from one system integrate enterprise is unpole with the supply chain should be controlled for release between the enterprise and third parties, information about the supply chain should be controlled for release between the enterprise and third parties, information may be exchanged between the enterprise and its suppliers, developers, system integration, external systems exchice providers and enter (TOT) related exercise providers. The controlled release of enterprise information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other ICTOT-related providers. Specifying the requirements and how information from set introduction may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other ICTOT-related service providers. Specifying the requirements as the interval of the service providers and the service providers and other ictors. The service should represent the correct of some service providers and the service providers and the service service interval of the service service services. The service should represent the correct of sould ensure that be controlled information is communicated to various participants in the supply chain service should specify unious source and destination points for information about systems and systems components, acquisition details, and delivery is considered metadata and may require proprised protections. Enterprises should specify vario	Functional  Functional  Functional	Equal Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement— Access Control Lists (ACLs)  Object Security Attributes  Cross Domain Authentication	DCH-03.3  NET-04  NET-04.2	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review firewall and router configurations to restrict connections between unbusted networks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to apply cybersecurity and/or data protection filters on metadata.  Mechanisms exist to ensure network architecture utilizes network	10	resulting from changes to the security stribution or usuajects and objects based on [Assignment- organization-defined rules governing the timing revocation of access authorizations].  Release information actistic of the system organization- defined system or system component provides or the system or system component provides or the system or system component provides are used to validate the appropriatency of the judgment organization-defined controls); and tip [Assignment organization-defined controls] are used to validate the appropriatency of the judgment of the judgment of the provides of the judgment of the provides or the judgment of the judgment organization organization-defined metadata].  Unsiquely identify and authenticate source and destination points by [Selection (one or more)-organization system; application; service; individually for information between different security comains; implement [Assignment organization-defined security or privacy policy filters] or information flows togration organization-defined security or privacy policy filters].
AC-4(17)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Validation of Metadata  Information Flow Enforcement   Validation of Metadata  Information Flow Enforcement   Position of Metadata	speements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM CAC Cards, etc.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transfered from one system integrate enterprises a not transfer the contract of the supply chain should be controlled for release between the enterprise and third parties. Information about the supply chain should be controlled for release between the enterprise and the supply chain should be controlled for release between the enterprise and the supply chain should be controlled for release between the enterprise and the supply chain should be controlled for release between the enterprise and the supply chain to a supplement of the supplement o	Functional  Functional  Functional	Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement— Access Control Lists (ACLs)  Object Security Attributes  Cross Domain Authentication  Metadata Validation	DCH-03.3  NET-04.2  NET-04.12	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and couter configurations to restrict connections between untrusted networks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely objects of the properties	10 10 10	resulting from changes to the security stribution or usual results of outsigned and objects based on [Assignment organization-defined rules governing the timing revocation of access authorizations].  Release information actistic of the system organization-defined rotation actistic of the system organization-defined controls), and the receiving (Assignment: organization-defined controls), and (Independent organization-defined information flow control passing organization-defined information flow control passing organization-defined information flow control passing organization-defined metadata).  Uniquely (desettify and authenticate occurs and destination points) (Selection) (one or more)-organization-defined metadata).  When transfering information between different security domains, implement (Assignment) controls organization-defined metadata).  Separate information flows logically or physically information information defined metadatament and/or techniques) to accomplish response to the control of the control
AC-4(1)  AC-4(17)  AC-4(19)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata	specements a requirement for contractors and sub-tier contractors to immediately return access credentials (e.g., tokens, PM CAC Cacid, s.et, 10 to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrate enterprise and the processes in place is supported. The contract is transferred from one system integrated requirements and processes in place integration about the supply chain should be controlled for release between the enterprise and third parties. Information may be exchanged between the enterprise and its suppliers, developers, system integrated extended and the controlled release of enterprise information may be exchanged between the enterprise and its suppliers, developers, system integrators, external systems extend providers. The controlled release of enterprise information protects against risks associated with disclosure.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other information may traverse a large supply chains to a broad set of stakeholders, including the enterprise information may traverse a large supply chains to a broad set of stakeholders, including the enterprise information and the various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other information service providers. Specifying the requirements systems service providers, and other information service providers. Specifying the requirements in the formation and flow down this requirement to relevant sub-ties contractors. Departments and agencies should refer to Accessed to the supply chain sequenter to relevant sub-ties contractors. Departments and agencies should refer to Accessed to the supply chain security and ensure that	Functional  Functional  Functional	Equal Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement— Access Control Lists (ACLs)  Object Security Attributes  Cross Domain Authentication	DCH-03.3  NET-04.2  NET-04.12	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and couter configurations to restrict connections between untrusted networks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely objects of the properties	10 10 10	resulting from changes to the society attributes or subjects and objects based on [Assignment-organization-defined rules governing the timing revocations of access subnorizations].  Release information outside of the system only (a) The receiving [Assignment organization-defined system or system components] provides defined system or system components] provides defined system or system components] provides the system or sy
AC-4(1)  AC-4(17)  AC-4(19)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Validation of Metadata  Information Flow Enforcement   Validation of Metadata  Information Flow Enforcement   Posterior of Metadata	specements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM oCA Cards, 4c, 10) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract it transferred from one system integrate enterprise is a notifier with the same personnel supporting integrated to the processes in place is a contract at the processes in place in the processes in the processes in place in the processes in the processes in the processes in the processes of the processes in the processes of the processes in the processes of the processes o	Functional  Functional  Functional	Equal Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement— Access Control Lists (ACLs)  Object Security Attributes  Cross Domain Authentication	DCH-03.3  NET-04.2  NET-04.12	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and couter configurations to restrict connections between untrusted networks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely objects of the properties	10 10 10	resulting from changes to the security stribution of usulpricts and objects based on [Assignment- organization-defined rules governing the time;  revocation of access authorizations].  Release information activit of the system conduction of the system or system component provides of the system or system component provides and system or system component provides are used to validate the appropriatence of the information defined controls]; and bij [Assignment: organization-defined controls] and bij [Assignment organization-defined controls] and bij [Assignment organization-defined controls] and bij [Assignment organization-defined controls] and [Assignment organization-defined controls] and [Assignment organization-defined information flow control based on [Assignment organization-defined information flow control based on [Assignment organization-defined metadata].  Uniquely identify and authemicate source and destination points by [Selection (nee or mnoc)-organization-defined metadata].  Uniquely identify and authemicate source and destination points by [Selection (nee or mnoc)-organization-defined metadata].  Uniquely identify and authemicate source and destination points by [Selection (nee or mnoc)-organization-defined metadata].  When transferring information between different security domains and or implement [Assignment: organization-defined recipiend (assignment: organization-defined recipiend (assignment) as a complaint organization defined metadata (assignment) and a complaints or defined recipiend (assignment) as a complaint organization-defined recipiend (assignment) as a complaint organization-defined recipiend (assignment) as a complaint organization-defined recipiend (assignment) as a complaint organization defined recipiend (assignment) as a complaint organization de
AC-4(1)  AC-4(17)  AC-4(19)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Validation of Metadata  Information Flow Enforcement   Validation of Metadata  Information Flow Enforcement   Posterior of Metadata	speements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM CAC Cards, 4c, 61) on the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrated restinguishes unsolve with the support shallow the controlled for release between the enterprise and third parties. Information about the supply chain should be controlled for release between the enterprise and third parties. Information may be exchanged between the enterprise and its suppliers, developers, system integration, sectionally accessed to the supply chain should be controlled for release between the enterprise and its integration, developers, system integration, section and the controlled release of enterprise information may traverse a large supply chain to a broad set of stakeholders. The controlled release of enterprise information protects against risks associated with disclosure.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its unsolvent sections. The controlled release of enterprise information protects against risks associated with disclosure service providers, and other ICTOT-related service providers. Specifying the requirements and how information to incommunicated to various participants in the supply chain. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant aburder controlled requirements and enterprise and the supply chain and information to a controlled requirement to relevant aburder controlled requirements and includes exclude information is communicated to various participants in the supply chain and under the providers and includes exclude information and agencies should represent the Nation's. The metadata and systems and systems and systems and systems and systems and systems a	Functional  Functional  Functional	Equal Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement— Access Control Lists (ACLs)  Object Security Attributes  Cross Domain Authentication	DCH-03.3  NET-04.2  NET-04.12	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and router configurations to restrict connections between untrusted networks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to apply cybersecurity and/or data protection filters on metadata.  Mechanisms exist to ensure network architecture utilizes network segmentation to isolates Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	10 10 10	resulting from changes to the security stribution or usual results of outsigned and objects based on [Assignment organization-defined rules governing the timing revocation of access authorizations].  Release information actistic of the system organization-defined rotation actistic of the system organization-defined controls), and the receiving (Assignment: organization-defined controls), and (Independent organization-defined information flow control passing organization-defined information flow control passing organization-defined information flow control passing organization-defined metadata).  Uniquely (desettify and authenticate occurs and destination points) (Selection) (one or more)-organization-defined metadata).  When transfering information between different security domains, implement (Assignment) controls organization-defined metadata).  Separate information flows logically or physically information information defined metadatament and/or techniques) to accomplish response to the control of the control
AC-4(1)  AC-4(17)  AC-4(19)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Validation of Metadata  Information Flow Enforcement   Validation of Metadata  Information Flow Enforcement   Posterior of Metadata	specements a requirement for contractors and sub-tier contractors to immediately return access credentials (e.g., takens, PM CAC Cacid, s.et, 10 to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transfered from one system integrator enterprise a not have with a contract and the contract of the supply chain should be controlled for release between the enterprise and third parties, information nay be exchanged between the enterprise and its suppliers, developers, system integrators, external systems exceive providers. The controlled release of enterprise and third parties, information may be exchanged between the enterprise and its suppliers, developers, system integrators, external systems exceive providers. The controlled release of enterprise information protects against risks associated with decideaux.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integrators, external system service providers. Set of stakeholders, including the enterprise and the various federal stakeholders, suppliers, developers, system integrators, external system service providers. Specifying the requirements and how on supplications of the providers of the stakeholders, including the enterprise and the various federal stakeholders, suppliers, developers, system integrators, external system service providers. And other ICTOT related service providers. Specifying the requirement and how of the providers of the stakeholders of the stakeholders of the stakeholders in the stakeholders of the stake	Functional  Functional  Functional	Equal Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement— Access Control Lists (ACLs)  Object Security Attributes  Cross Domain Authentication	DCH-03.3  NET-04.2  NET-04.12	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and router configurations to restrict connections between untrusted networks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to apply cybersecurity and/or data protection filters on metadata.  Mechanisms exist to ensure network architecture utilizes network segmentation to isolates Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	10 10 10	resulting from changes to the society attributes or subjects and objects based on [Assignment-organization-defined rules governing the timing revocations of access authorizations].  Release information outside of the system only (a) The resolving [Assignment organization-defined resolvent organization-defined controls] and [Assignment organization-defined controls] and between connected systems assessed on [Assignment organization-defined information flow control based on [Assignment organization-defined information flow control based on [Assignment organization-defined metadata].  Uniquely identify and authenticate source and destination points by [Selection (nee or more): organization-defined metadata].  When transferring information between different security domains, implement [Assignment: organization-defined record accessed information flows togically or physical using [Assignment: organization-defined required security or privacy policy filters] on metadata.  Separate information flows togically or physical using [Assignment: organization-defined required separations by byte or information].  a. Identify and document [Assignment: organization-defined required separations by byte or information].
AC-4(17)  AC-4(19)  AC-4(21)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Validation of Metadata  Information Flow Enforcement   Validation of Metadata Information Flow Enforcement   Validation of Metadata Information Flow Enforcement   Validation of Metadata Information Flow Information F	speements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM or CAC cards, etc.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract its transferd from one system integrate enterprise a not the supply chain should be controlled for release between the enterprise and third parties, information about the supply chain should be controlled for release between the enterprise and third parties, information may be exchanged between the enterprise and its suppliers, developers, system integration, external systems envice providers, and other ICTOT-related envice providers. The controlled release of enterprise information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other ICTOT-related providers. Specifying the requirements and how information from a stordered should ensure that only the required information is communicated to various participants in the supply chain. Enterprises should require their prime contractors to implement this control and flow down that requirement to relevant as the contractors. Departments and agencies should refer to Accordal F to intellegent and the storders and the storders and the storders and the storders. The storders are storders and the storders are storders and the	Functional  Functional  Functional  Functional	Equal Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement— Access Control Lists (ACLs)  Object Security Attributes  Cross Domain Authentication  Metadata Validation	DCH-03.3  NET-04.2  NET-04.12  NET-04.13	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and router configurations to restrict connections between untrusted networks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to apply cybersecurity and/or data protection filters on metadata.  Mechanisms exist to ensure network architecture utilizes network segmentation to isolates Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	10 10 10 10	resulting from changes to the security stribution or usual resulting from changes to the security stribution or subjects and objects based on [Assignment organization-defined rules governing the timing revocation of access authorizations].  Release information actistic of the system organization-defined system or system component provides and the system or system component provides are used to validate the appropriatency of the [Assignment organization-defined controls]; and toll [Assignment organization-defined controls] and toll [Assignment organization within the system and between connected systems based on [Assignment organization-defined information flow control policies].  Uniquely identify and authenticate source and destination points by [Selection (noe or more): organization-defined metadata].  When transferricg information between different security domains, implement [Assignment organization-defined metadata].  When transferricg information between different security domains, implement [Assignment organization-defined metadata].  Separate information flows togically or physically approached the significancy organization-defined metadata in the significancy organization defined metadata in the significancy org
AC-4(1)  AC-4(17)  AC-4(19)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Validation of Metadata  Information Flow Enforcement   Validation of Metadata Information Flow Enforcement   Validation of Metadata Information Flow Enforcement   Validation of Metadata Information Flow Information F	speements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM CAC Cards, etc.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transfered from one system integrate enterprises a not the supply chain should be controlled for release between the enterprise and third parties. Information about the supply chain should be controlled for release between the enterprise and third parties. Information may be exchanged between the enterprise and its suppliers, developers, system integration, sectional systems envice providers, and other ICTOT-related service providers. The controlled releases of enterprise information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integrators, external systems service providers, and other ICTOT-related providers. Specifying the requirements and how information from six entrode should ensure that only the requirement of evelopers, system integrators, external systems service providers, and other ICTOT-related service providers. Specifying the requirements of events and the service providers and other ICTOT-related service providers. Specifying the requirements of events and the service providers and the service providers and other ictoTOT-related service providers. Specifying the requirement to events and between the control of the service services and the service providers and services	Functional  Functional  Functional  Functional	Equal Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement— Access Control Lists (ACLs)  Object Security Attributes  Cross Domain Authentication  Metadata Validation	DCH-03.3  NET-04.2  NET-04.12  NET-04.13	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and router configurations to restrict connections between untrusted networks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to apply cybersecurity and/or data protection filters on metadata.  Mechanisms exist to ensure network architecture utilizes network segmentation to isolates Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.  Mechanisms exist to check the validity of information inputs.	10 10 10 10	resulting from changes to the society attributes or subjects and objects based on [Assignment-organization-defined rules governing the timing revocations of access authorizations].  Release information outside of the system only (a) The resolving [Assignment organization-defined resolvent organization-defined controls] and [Assignment organization-defined controls] and between connected systems assessed on [Assignment organization-defined information flow control based on [Assignment organization-defined information flow control based on [Assignment organization-defined metadata].  Uniquely identify and authenticate source and destination points by [Selection (nee or more): organization-defined metadata].  When transferring information between different security domains, implement [Assignment: organization-defined record accessed information flows togically or physical using [Assignment: organization-defined required security or privacy policy filters] on metadata.  Separate information flows togically or physical using [Assignment: organization-defined required separations by byte or information].  a. Identify and document [Assignment: organization-defined required separations by byte or information].
AC-4(1)  AC-4(17)  AC-4(19)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Validation of Metadata  Information Flow Enforcement   Validation of Metadata Information Flow Enforcement   Validation of Metadata Information Flow Enforcement   Validation of Metadata Information Flow Information F	specements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM CAC Cacid, etc.) to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract it transferred from one system integrate enterprise and the support integrated processes in place in a contract of the support of th	Functional  Functional  Functional  Functional	Equal Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement- Access Control Lists (ACLs)  Object Security Attributes  Cross Domain Authentication  Metadata Validation	DCH-03.3  NET-04.2  NET-04.12  NET-04.13	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and router configurations to restrict connections between untrusted rehvorks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enflore defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to apply cybersecurity and/or data protection filters on metadata.  Pechanisms exist to entoure network architecture utilizes network aggrenation for its isolate to chronology Assets, Applications and/or Services (TAAS) to protect from other network resources.  Mechanisms exist to check the validity of information inputs.  Mechanisms exist to check the validity of information inputs.	10 10 10 10	resulting from changes to the security stributes or subjects and objects based on [Assignment organization-defined rules governing the timing revocations of access authorizations].  Assignment organization defined the system organization defined system or system component provides of the program of the pr
AC-4(17)  AC-4(17)  AC-4(19)  AC-4(21)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Validation of Metadata  Information Flow Enforcement   Commandation Flow Enforcement   Commandation Flow Enforcement   Power   Information Flow Enforcement   Power   Informatio	specements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM oCA Cards, 4c., 10 to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract it transfered from one system integrate enterprise is unpole with the superprise intermed to contract its transfered from one system integrated enterprises and the supply chain should be controlled for release between the enterprise and third parties. Information may be exchanged between the enterprise and its suppliers, developers, system integration, and the suppliers of the suppliers of the suppliers of the suppliers of the suppliers. The controlled release of enterprise information may be exchanged between the enterprise and its suppliers, developers, system integration.  Supply chain information protects against risks associated with disclosure.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and it various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other ICTOT-related service providers. Specifying the requirements and how intermediated to the supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other ICTOT-related service providers. Specifying the requirements and how intermediation in the supply chain integrators, and the ICTOT-related service providers. Specifying the requirement that how intermediated integration is control as a supply chain integrators. The providers that the supply chain is control as a supply chain integrators in the supply chain integrators. In the supply chain is control as a supply chain is control as a supply chain integrators. The providers is control	Functional  Functional  Functional  Functional  Functional	Equal Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement - Access Control Lists (ACLs)  Object Security Attributes  Cross Domain Authentication  Metadata Validation  Network Segmentation (macrosegementation)	DCH-03.3  NET-04.2  NET-04.12  NET-04.13  NET-04.13	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and router configurations to restrict connections between untrusted networks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to apply cybersecurity and/or data protection filters on metadata.  Mechanisms exist to ensure network architecture utilizes network segmentation to isolates Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.  Mechanisms exist to check the validity of information inputs.	10 10 10 10 5	resulting from changes to the security stribution of usulpricts and objects based on [Assignment- organization-defined rules governing the timing revocation of access authorizations].  Release information activities of the system condition of the system or system component provides of the program of the p
AC-4(1)  AC-4(17)  AC-4(19)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Validation of Metadata  Information Flow Enforcement   Validation of Metadata Information Flow Enforcement   Validation of Metadata Information Flow Enforcement   Validation of Metadata Information Flow Information F	specements a requirement for contractors and sub-tier contractors to immediately return access credentials (e.g., Lokens, PR) CAC Cacid, s.et, 10 to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transfered from one system integrator enterprise a notification in a "badge flipping" situation, a contract is transfered from one system integrator enterprise as a notification in a secondary of the contract is transfered from one system integrator enterprises and its suppliers, developers, system integrators, askential system sense personnel supporting.  Integration may be exchanged between the enterprise and its suppliers, developers, system integrators, external systems excite providers. In determining the controlled release of enterprise information may traverse a large supply chains to a broad set of stakeholders, including the enterprise information may traverse a large supply chains to a broad set of stakeholders, including the enterprise information may traverse a large supply chains to a broad set of stakeholders, including the enterprise information may traverse a large supply chains to a broad set of stakeholders, including the enterprise information may traverse a large supply chains to a broad set of stakeholders, including the enterprise information may traverse a large supply chains to a broad set of stakeholders, including the enterprise information may traverse a large supply chains to a broad set of stakeholders, including the enterprise information in the state of the stakeholders, including the enterprise providers. Specifying the requirements and though the supply chains to a state of the state o	Functional  Functional  Functional  Functional	Equal Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement- Access Control Lists (ACLs)  Object Security Attributes  Cross Domain Authentication  Metadata Validation	DCH-03.3  NET-04.2  NET-04.12  NET-04.13	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and router configurations to restrict connections between untrusted rehvorks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enflore defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to apply cybersecurity and/or data protection filters on metadata.  Pechanisms exist to entoure network architecture utilizes network aggrenation for its isolate to chronology Assets, Applications and/or Services (TAAS) to protect from other network resources.  Mechanisms exist to check the validity of information inputs.  Mechanisms exist to check the validity of information inputs.	10 10 10 10	resulting from changes to the security attributes or subjects and objects based on [Assignment- organization-defined rules governing the timing revocations of access authorizations].  Release information adulties of the system only [Assignment processing of the system
AC-4(17)  AC-4(19)  AC-4(21)  AC-5	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Validation of Metadata  Information Flow Enforcement   Commandation Flow Enforcement   Commandation Flow Enforcement   Power   Information Flow Enforcement   Power   Informatio	specements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM, CAC Cacid, s.et, 10 to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transfered from one system integrator enterprise a not the view to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transfered from one system integrator enterprise and the supplication may be exchanged between the enterprise and its suppliers, developers, system integrators, access the system of the process of the controlled release of enterprise information may be exchanged between the enterprise and its suppliers, developers, system integrators, external systems excise providers. But the CTIOT-related service providers. But the controlled release of enterprise information protects against risks associated with disclosure.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and the various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other incompanies of the controlled release of enterprise information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and the various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other incompanies systems service providers. Specifying the requirements and how some service providers, and other incompanies of the control of the c	Functional  Functional  Functional  Functional  Functional	Equal Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement— Access Control Lists (ACLs)  Object Security Attributes  Cross Domain Authentication  Metadata Validation  Network Segmentation (macrosegementation)  Input Data Validation for	DCH-03.3  NET-04.2  NET-04.12  NET-04.13  NET-04.13	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and router configurations to restrict connections between untrusted rehvorks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enflore defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to apply cybersecurity and/or data protection filters on metadata.  Pechanisms exist to entoure network architecture utilizes network aggrenation for its isolate to chronology Assets, Applications and/or Services (TAAS) to protect from other network resources.  Mechanisms exist to check the validity of information inputs.  Mechanisms exist to check the validity of information inputs.	10 10 10 10 5	resulting from changes to the security stribution of usulpricts and objects based on [Assignment- organization-defined rules governing the timing revocation of access authorizations].  Release information activities of the system condition of the system or system component provides of the program of the p
AC-3(9)  AC-4  AC-4(17)  AC-4(19)  AC-4(21)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Validation of Metadata  Information Flow Enforcement   Commandation Flow Enforcement   Commandation Flow Enforcement   Power   Information Flow Enforcement   Power   Informatio	speements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM CAC Cards, 4c, 61) on the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract its transferd from one system integrate enterprise is unplicitly and processes in place in contract its transferd from one system integrate enterprises a not its suppliers, developers, system integration, sectional systems among providers, and other integrations, developers, system integration, external systems envice providers, and other it (TOT) -related envice providers, and controlled releases of enterprise information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal stakeholders, suppliers, developers, system integrators, external systems exercise providers. And other it (TOT) -related exercise providers. Specifying the requirements and how information from a storticed should ensure that only the required information is communicated to various participants in the supply chain. Enterprises should require their prime contractors to implement this control information for set incrediments of the set in the stort of the stortice should ensure at the director of the stortice should ensure at the director of the stortice should ensure at the director of the stortice should ensure that of the stortice should ensure at the director of the stortice should ensure that the control of the stortice should ensure that the stortice should expect the stortice should expect the stortice should expect the stortice should expect the supply chain societies with the Stortice should expect to their supply chain societies with the Stortice should expect to their supply chain information about systems and system components, equivalent of the stortice should expect to their supply chain societies and incrediment to evidence and may require appropri	Functional  Functional  Functional  Functional  Functional	Equal Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement— Access Control Lists (ACLs)  Object Security Attributes  Cross Domain Authentication  Metadata Validation  Network Segmentation (macrosegementation)  Input Data Validation for	DCH-03.3  NET-04.2  NET-04.12  NET-04.13  NET-04.13	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and router configurations to restrict connections between untrusted networks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to spiply cybersecurity and/or data protection filters on metadata.  Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from order network resources.  Mechanisms exist to check the validity of information inputs.  Mechanisms exist to check the validity of information inputs.	10 10 10 10 5	resulting from changes to the security stribution of usulpricts and objects based on [Assignment- organization-defined rules governing the timing revocation of access authorizations].  Release information actistic of the system conjugation of the process of the
AC-3(9)  AC-4(17)  AC-4(17)  AC-4(19)  AC-5	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Validation of Metadata  Information Flow Enforcement   Commandation Flow Enforcement   Commandation Flow Enforcement   Power   Information Flow Enforcement   Power   Informatio	specements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM, CAC Cacid, s.et, 10 to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transfered from one system integrator enterprise a not the view to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transfered from one system integrator enterprise and the supplication may be exchanged between the enterprise and its suppliers, developers, system integrators, access the system of the process of the controlled release of enterprise information may be exchanged between the enterprise and its suppliers, developers, system integrators, external systems excise providers. But the CTIOT-related service providers. But the controlled release of enterprise information protects against risks associated with disclosure.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and the various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other incompanies of the controlled release of enterprise information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and the various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other incompanies systems service providers. Specifying the requirements and how some service providers, and other incompanies of the control of the c	Functional  Functional  Functional  Functional  Functional	Equal Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement— Access Control Lists (ACLs)  Object Security Attributes  Cross Domain Authentication  Metadata Validation  Network Segmentation (macrosegementation)  Input Data Validation for	DCH-03.3  NET-04.2  NET-04.12  NET-04.13  NET-04.13	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Nechanisms exist to design, implement and review frewall and router configurations to restrict connections between untrusted retworks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enflore defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to spaply cybersecurity and/or data protection filters on metadata.  Nechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or Services (TAAS).  Chyptographic mechanisms exist to implement strong cryptography and	10 10 10 10 5	resulting from changes to the security stribution of usulpricts and objects based on [Assignment- organization-defined rules governing the timing revocation of access authorizations].  Release information actistic of the system conjugation of the process of the
AC-3(9)  AC-4(1)  AC-4(17)  AC-4(19)  AC-4(21)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Population Information Flow Enforcement   Population Information Flow Enforcement   Physical or Logical Separation of Information Flows  Separation of Duties  Separation of Duties	specements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM oCA Cards, 4c., 10 to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrate enterprise is a notificary with the supply chain should be controlled for release between the enterprise and third parties, information about the supply chain should be controlled for release between the enterprise and third parties, information may be exchanged between the enterprise and its suppliers, developers, system integrators, desirable information may be exchanged between the enterprise and its suppliers, developers, system integrators, desirable size information may be exchanged between the enterprise and its suppliers, developers, system integrators, catenal system service providers and other ICTOT-related service providers. The controlled release of enterprise information protects against risks associated with disclosure.  Supply chain information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and it various federal stakeholders, suppliers, developers, system integrators, external system service providers, and other ICTOT-related service providers. Specifying the requirements and how information to externed should ensure that only the required information is communicated to various participants in the supply chain. Enterprises should require their prime contractors to implement this control should ensure that only the required information is communicated to various and may require approprise protections. Enterprises and includes activities within the SDC. For example, information about systems and system components, acquisition details, and delivery is considered metadata and may require proprise protections. Enterprises a provider providers and destination points for information about the supply	Functional  Functional  Functional  Functional  Functional	Equal  Equal  Equal  Equal	Authorizations  Controlled Release  Data Flow Enforcement— Access Control Lists (ACLs)  Object Security Attributes  Cross Domain Authentication  Metadata Validation  Network Segmentation (macrosegementation)  Input Data Validation for	DCH-03.3  NET-04.12  NET-04.12  NET-04.13  NET-04.13  CHG-04.3	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and router configurations to restrict connections between untrusted networks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to spiply cybersecurity and/or data protection filters on metadata.  Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from order network resources.  Mechanisms exist to check the validity of information inputs.  Mechanisms exist to check the validity of information inputs.	10 10 10 10 5 5 5	resulting from changes to the security stribution of usulpricts and objects based on [Assignment- organization-defined rules governing the timing revocation of access authorizations].  Release information activit of the system condition of the control of the received (assignment organization-defined controls) and (b) feesing the control of the contr
AC-3(9)  AC-4  AC-4(17)  AC-4(19)  AC-4(21)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Validation of Metadata  Information Flow Enforcement   Commandation Flow Enforcement   Commandation Flow Enforcement   Power   Information Flow Enforcement   Power   Informatio	specements a requirement for contractors and sub-ter contractors to immediately return access credentials (e.g., tokens, PM oCA Cards, 4c., 10 to the enterprise. Enterprises must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract it transfered from one system integrate enterprise a notification in the processes in place in the contract of the prompt of the processes in place in the processes in the processes in the processes in the processes of extending system service providers, and other ICTOT-related exivity or providers, and the various federal state devices providers. The controlled release of enterprise information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and it various federal stateholders, suppliers, developens, system integrators, external system service providers, and other ICTOT-related providers. Specifying the requirements and how intermediate and the providers and the ICTOT-related providers. Specifying the requirements and how intermediate the supply chain integrators, and the ICTOT-related service providers. Specifying the requirements and how intermediate the supply chains. Cerebrate state of the providers is specifying the requirement and how intermediate the supply chain integrators. As a supply chain integrator in the supply chain integrators are supply chain integrators. The providers is a supply chain integrator in the supply chain integrators are supply chain integrators. The providers is a supply chain integrator in the supply chain integrators are supply chain integrators. The providers in the supply chain integrator in the supply chain integrators are supply chain integrators. The providers in the supply chain integrators in the supply chain integrators in the sup	Functional  Functional  Functional  Functional  Functional	Equal Equal Equal	Authorizations  Controlled Release  Data Flow Enforcement— Access Control Lists (ACLs)  Object Security Attributes  Cross Domain Authentication  Metadata Validation  Network Segmentation (macrosegementation)  Input Data Validation  Dual Authorization for Change	DCH-03.3  NET-04.2  NET-04.12  NET-04.13  NET-04.13	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and router configurations to restrict connections between untrusted networks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to spply cybersecurity and/or data protection filters on metadata.  Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.  Mechanisms exist to check the validity of information inputs.  Mechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or Services (TAAS).  Crystographic mechanisms exist to implement storng cryptography and security protocols to safeguard sensitive/regulated data during	10 10 10 10 5	resulting from changes to the security stribution of usulpricts and objects based on [Assignment- organization-defined rules governing the timing revocation of access authorizations].  Release information actistic of the system concentration of the program of the program of the process of the program of the process of the program of the process of the program of t
AC-3(9)  AC-4(1)  AC-4(17)  AC-4(19)  AC-4(21)	Revocation of Access Authorizations  Access Enforcement   Controlled Release  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Metadata  Information Flow Enforcement   Population Information Flow Enforcement   Population Information Flow Enforcement   Physical or Logical Separation of Information Flows  Separation of Duties  Separation of Duties	specements a requirement for contractors and sub-tier contractors to immediately return access credentials (e.g., Lotens, PR) CAC Cacid, s.et, 10 to the enterprise. Enterprise must also have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transfered from one system integrated respirate a nonther with the same personnel supporting. International contractions are provided from the supply chain is about a become with the supply chain and the supply chain to a broad set of stakeholders, including the enterprise and its various federal taskeholders, suppliers, developers, system integrators, and the suppliers information may traverse a large supply chain to a broad set of stakeholders, including the enterprise and its various federal taskeholders, suppliers, developers, system integrators, external system extensive and its various federal taskeholders, suppliers, developers, system integrators, external system suppliers, developers, system integrators, external system submitted for the suppliers, developers, system integrators, external system submitted for the suppliers, developers, system integrators, external system submitted for the suppliers and supply chain. This is so that enterprises have stability of reformatio	Functional  Functional  Functional  Functional  Functional	Equal  Equal  Equal  Equal	Authorizations  Controlled Release  Data Flow Enforcement— Access Control Lists (ACLs)  Object Security Attributes  Cross Domain Authentication  Metadata Validation  Metadata Validation  Input Data Validation  Dual Authorization for Change	DCH-03.3  NET-04.12  NET-04.12  NET-04.13  NET-04.13  CHG-04.3	protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  Mechanisms exist to design, implement and review frewall and router configurations to restrict connections between untrusted networks and internal systems.  Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.  Automated mechanisms exist to spply cybersecurity and/or data protection filters on metadata.  Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.  Mechanisms exist to check the validity of information inputs.  Mechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or Services (TAAS).  Crystographic mechanisms exist to implement storng cryptography and security protocols to safeguard sensitive/regulated data during	10 10 10 10 5 5 5	resulting from changes to the security attributes or subjects and objects based on [Assignment- organization-defined rules governing the timing revocations of secs authorizations].  Palesses information adulties of the system only. In the case of the system of the system of the system of the system or system component provides of the system or system component provides or system or system component provides or system or sy



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM	STRM	SCF Control	SCF#	Secure Controls Framework (SCF)	Strength of Relationship	Notes (optional)
		NIST SP 800-161 R1 Supplemental C-SCRM Guidance  The enterprise should ensure that an appropriate separation of duties is established for decisions that require	Rationale	Relationship			Control Description  Mechanisms exist to implement and maintain Separation of Duties (SoD)	/ontionall	a. Identify and document [Assignment:
AC-5	Separation of Duties	the acquisition of both information system and supply chain components. The separation of duties helps to ensure that adequate protections are in Jace for components entering the enterprise's supply chain, such as denying developers the privilege to promote code that they work form developerant to production environments. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-field contractors. Departments and sunches should refer for Aspecials of It onlinement this suidance in accordance with Executive Order 14028.	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	to prevent potential inappropriate activity without collusion.	5	a. Identify and document (Assignment: organization-defined duties of individuals requiring separation); and b. Define system access authorizations to support separation of duties.
AC-6	Least Privilege	For C-SCRM supplemental guidance, see control enhancements. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, improving the Nation's Cybersecurity.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
AC-6	Least Privilege	For C-SCRM supplemental guidance, see controt enhancements. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, improving the Nation's Cybersecurity.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (IAC) permissions that conform to the principle of "least privilege."	5	
AC-6(6)	Least Privilege   Privileged Access by Non organizational Users	Enterprises should ensure that protections are in place to prevent non-enterprise users from having privileged access to enterprise supply chain and related supply chain information. When enterprise users include independent consultants, suppliers, developens, system insignators, extend systems envice providers, and other ICTOT-related service providers, relevant access requirements may need to use least privilege mechanisms to precisely define what information and/or components are accessible, for what duration, at what frequency, using what access methods, and by whom. Understanding what components are critical and on-critical can all fundestanding the world default that may need to be defined regarding least privilege.	Functional	Equal	Privileged Access by Non Organizational Users	IAC-05.2	Mechanisms exist to prohibit privileged access by non-organizational users.	10	Prohibit privileged access to the system by non- organizational users.
AC-17	Remote Access	Ever more frequently, supply chains are accessed remotely. Whether for the purpose of development, maintenance, or the operation of information systems, enterprises should implement secure remote access mechanisms and allow remote access only to vetted personnel. Remote access to an enterprise? supply chain fincluding distributed software development environments) should be limited to the enterprise or contractor personnel and only if and as required to perform their tasks. Remote soccess requirements—auch using a secure VMV, employing multi-factor authentication, or limiting access to consense the contraction of the contracti	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and     b. Authorize each type of remote access to the system prior to allowing such connections.
AC-17(6)	Remote Access   Protection of Mechanism Information	seacified business hours or from seacified seatrantic locations — must be properly defined in asserments. Enterprises should ensure that detailed requirements are properly defined and that access to information regarding the information system and supply chain is protected from unauthorized use and disclosure. Since supply chain data and metadata disclosure or access can have significant implications for an enterprise's mission processes, approprised measures must be taken to verb of the supply chain and personnel processes to ensure that adequate protections are implemented. Ensure that remote access to such information is included in requirements.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	Protect information about remote access mechanisms from unauthorized use and disclosure.
AC-18	Wireless Access	An enterprise a supply chain may include stelese infrastructure. But supports supply chain legistics (e.g., sedio-frequency (extraction) extractions are considered in the sedio-frequency (extraction) extractions are supply chain as they are moved from one location to another, whether systems/components traverse the supply chain as they are moved from one location to another, whether within the entarprise is own enricoment 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, a well as legistics technologies and metadats used during the information systems and components.	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	shlooin te. d., within trackins ensors). The enterories should exhibitive define appropriate wireless access An enterpries a supply chain may include wireless infrastructure that supports supply chain logistical (e.g., radio-frequency identification device [RFID] support, software call home features). Supply chain systems/components traverse the supply chain as the year enwel from one location to another, whether within the entarprise'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, a well as logistics technologies and metadats used during the information systems and components, a well as logistics technologies and metadats used during	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	absoint is d.e., within tracking sensors). The enterories should exilicitly define appropriate wireless access The use of mobile devices (e.g., laptops, ablete, e-readers, namphones, namwatches) has become common in the supply chain. They are used in direct support of an enterprise's operations, as well as tracking, supply chain foliagitics, data as information systems, and components that travense 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 handhed units in FISO for tracking commonents that travente the supply chain components. An example of such as Interpretable commonents are the supply chain care.	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' otermal information systems include those of suppliers, developers, system integrations, external system sencine providers, and other CIOT behalted sencine providers. Utilities in an ocquirer'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-lier contractors.	Functional	Equal	Use of External Information Systems	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
AC-20(1)	Use of External Systems   Limits on Authorized Use	This enhancement helps limit exposure of the supply chain to the systems of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Equal	Limits of Authorized Use	DCH-13.1	Mechanisms exist to prohibit external parties, including Technology Assets, Applications and/or Services (TAS), from storing, processing and transmitting data unless authorized incliviously first: (1) Verifying the implementation of required security controls; or (2) Retaining a processing agreement with the entity hosting the external TAAS.	10	Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after: (a) Verification of the implementation of controls or the external system as specified in the orthorized access and controls or orthorized to the controls of orthorized to the controls or the external system as specified in the orthorized to controls or orthorized to controls or orthorized ortho
AC-20(3)	Use of External Systems   Non-organizationally Owned Systems — Restricted Use	Devices that do not belong to the enterprise (e.g., bring your own device [EYOD] policies) increase the enterprise's exposure to cyber security risks throughout the supply claim. This includes devices used by supplies, developer, by other integrations, covered up your service productions by the production of supplies, developer, by other integrations, covered up you are producted to the production of supplies, developer, by the production of the production of the production of supplies that the production of the production of the production of and make a risk-based decision as to whether it will allow the use of such devices or furnish devices. Thereprises should intrinsif devices to them connecting the promonet who present unacceptable levels of risk.	Functional	Equal	Non-Organizationally Owned Systems / Components / Devices	DCH-13.4	Mechanisms exist to restrict the use of non-organizationally owned Technology Assets, Applications and/or Services (TAAS) to process, store or transmit organizational information.	10	Restrict the use of non-organizationally owned systems or system components to process, store, or transmit organizational information using [Assignment: organization-defined restrictions].
AC-21	Information Sharing	Staring information within the supply chain can help manage cybersecurity risks throughout the supply chain. This information may include vulnerabilities, threats, the criticality of systems and components, or delivery information. This information chaining should be carefully managed to ensure that the information is only accessible to authorized individuals within the enterprise's supply chain. Enterprises should clearly define boundaries for information chaining with respect to semporal, informational, contractus, security, access, system, and other requirements. Enterprises should monitor and review for unintentional or intentional information sharing with this supplex chains certified. Including information sharing with suppliers.	Functional	Intersects With	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	5	a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [Assignment: organization- defined information sharing circumstances where user discretion is required]; and b. Employ (Assignment: organization-defined
AC-21	Information Sharing	Dating information within the supply chain can help malage operacounty into the topological state throughout the supply chain. This information may include vulnerabilities, threats, the criticality of systems and components, or delivery information may include vulnerabilities, threats, the criticality of systems and components, or delivery information. This information chaining whom to be carefully managed to ensure that the information is only accessible to authorized individuals within the enterprise's supply chain. Enterprises should clearly define boundaries for information of haring with respect to temporal, informational, contractus, security, access, system, and other requirements. Enterprises should into monitor and review for unintentional or intentional information sharing with the activities. Including information sharing with subsoilers.	Functional	Intersects With	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5	5. Enable authorized users to determine whether access authorized users to determine whether access authorized ions assigned to a sharing partner match the information's access and use restrictions for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and b. Emolov [Assignment: organization-defined].
AC-22	Publicly Accessible Content	Within the C-SCRM context, publicly seekselbe 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	D. Emigor Possentine and Section of Section (Section 1) and Section (Section 1
AC-23	Data Mining Protection	Enterprises should require their prime contractors to implement this control as part of their insider threat activities and flow down this requirement to relevant sub-lier contractors.	Functional	Intersects With	Data Mining Protection	DCH-16	Mechanisms exist to protect data storage objects against unauthorized data mining and data harvesting techniques.	5	Employ [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to detect and protect against unauthorized data mining.
AC-23	Data Mining Protection	Enterprises should require their prime contractors to implement this control as part of their insider threat activities and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purposely) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual oblications.	5	Employ [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to detect and protect against unauthorized data mining.
AC-24	Access Control Decisions	Enterprises should assign access control decisions to support authorized access to the supply chair. Ensure that if a system integrator or external service provider is used, there is consistency in access control decision requirements and how the requirements are implemented. This may require defining such requirements in service—level agreements, in many cases as part of the upfront relationship established between the enterprise and systems allowed previous discovered in the provider of	Functional	Intersects With	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	5	[Selection: Establish procedures: Implement mechanisms] to ensure [Assignment: organization-defined access control decisions] are applied to each access request prior to access enforcement.
AT-1		Enterprises should designate a specific official to manage the development, documentation, and dissemination of the training policy and procedures, including CSCM and not be-based specific training for those with supply chain responsibilities. Enterprises should integrate cybersecurity supply chain risk management training and swareness into the security training and awareness policy. CSCMM training should taget both the enterprise and 1st contractors. The policy should ensure that supply-chain dybersecurity role- based training is required for those individuals or functions that touch or impact the supply chain, such as the full mental contraction covers consistions caused that locations, seath endinessing coversm management.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned internals or siligational changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or rotes]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that:  [in) Addresses purpose, scope, rotes,
AT-1	Policy and Procedures	Enterprises should designate a specific official to manage the development, documentation, and dissemination of the training policy and procedures, including C-SCMP and role beads apscific training for those will supply chain responsibilities. Enterprises should integrate cybersecurity supply chain risk management training and ownerness to the security statistic and ownerness policy. C-SCMP starning should management training and ownerness to the security starting and ownerness policy. C-SCMP starning should be added training a required for those individuals or functions that touch or impact the supply chain, such as the information system owner, acquisition, such or hash totals to write enterprise corresponding such control of the supply of the supply chain totals to extend enterprise corresponding such control of the supply of the supply of the supply chain such as the submarked on system owner. Acquisition, such or hash totals to extend enterprise corresponding such control of the supply of the s	Functional	Subset Of	Cybersecurity & Data Protection-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/Dusiness process-level; System-level] awareness and training policy that:  (a) Addresses purpose, scooe, roles.
AT-1		Enterprises should designate a specific official to manage the development, documentation, and dissemination of the training policy and procedures, including CSCMP and role-based specific training for those with supply chain responsibilities. Enterprises should integrate cybersecurity supply chain risk management training and awaveness tink the security training and awaveness policy. CSCRM training should taget 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 bouch or impact the supply chain, such as the information scales movers, acculation, sucody chain lossists, visite entirelement, concern management. If,	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	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 this (a) Addresses purpose, scope, roles.



FDE#	FDE Name	Focal Document Element (FDE) Description NIST SP 800-161 R1 Supplemental C-SCRM Guidance	STRM	STRM	SCF Control	SCF#	Secure Controls Framework (SCF)	Strength of Relationship	Notes (optional)
		NIST SP 800-161 R1 Supplemental C-SCRM Guidance	Rationale	Relationship			Control Description  Mechanisms exist to provide all employees and contractors appropriate	(ontional)	a. Provide security and privacy literacy training to
AT-2	Literacy Training and Awareness	C-SCRM-specific supplemental guidance is provided in the control enhancements. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, improving the Nation's Cybersecurity.	Functional	Equal	Cybersecurity & Data Protection Awareness Training	SAT-02	awareness education and training that is relevant for their job function.	10	system users (including managers, senior executives, and contractors):  1. As part of initial training for new users and [Assignment: organization-defined frequency] thereafter; and
AT-2(1)	Literacy Training and Awareness   Practical Exercises	Enterprises should provide practical exercises in literacy training that simulate supply chain cybersecurity events and incidents. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-level contractors.	Functional	Intersects With	Simulated Cyber Attack Scenario Training	SAT-02.1	Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.	5	When required by system changes or following     Provide practical exercises in literacy training that simulate events and incidents.
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-2(3)	Literacy Training and Awareness   Social Engineering and Mining	Enterprises should provide literacy training on recognizing and reporting potential and actual instances of supply chain-related social engineering and social mining. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-level contractors.	Functional	Equal	Social Engineering & Mining	SAT-02.2	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.	10	Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.
AT-2(4)	Literacy Training and Awareness   Suspicious Communications and Anomalous System Behavior	Provide literacy training on recognizing suspicious communications or anomalous behavior in enterprise supply chain systems. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-level contractors.	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malwave to recognize suspicious communications and anomalous behavior.	5	Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using [Assignment. organization-defined indicators of malicious code].
AT-2(5)	Literacy Training and Awareness   Advanced Persistent Threat	Provide literacy training on recognizing suspicious communications on an advanced pensistent threat (APT) in the enterprise's supply chain. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-level contractors.	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomatious behavior.	5	Provide literacy training on the advanced persistent threat.
AT-2(6)	Literacy Training and Awareness   Cyber Threat Environment	Provide literacy training on cyber threats specific to the enterprise's supply chain environment. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-level contractors	Functional	Equal	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybensecurity and data protection awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	10	(a) Provide literacy training on the cyber threat environment; and (b) Reflect current cyber threat information in system operations.
AT-3	Role-based Training	Addressing oyler supply chain risks throughout the acquisition process is essential to performing C-SCRM effectively. Personnel what or part of the acquisition workfore require training no 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 raining requirements should be talked to be considered by the proposable for conducting thest assessments. Responding to threats and identified risks requires training in counterintelligence awareness and reporting. Enterprises should ensure that developeers receive training on security endedoment practices as well as the use of volvierability scanning	Functional	Intersects With	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection- related training:  (1) Before authorizing access to the system or performing assigned duties;  (2) When required by system changes; and  (3) Annually thereafter.	5	a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment-organization- defined roles and responsibilities]: 1. Before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency]
AT-3(2)	Rote-based Training   Physical Security Controls	C-SCRM is impacted by a number of physical security mechanisms and procedures within the supply chain, such as manufacturing, shipping, receiving, physical access to facilities, inventory management, and were housing. Enterine and system integrator personnel who provide development and operational support to see the providence of t	Functional	Intersects With	Rote-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection- related training:  (1) Before authorizing access to the system or performing assigned duties;  (2) When required by system changes; and  (3) Annually thereafter.	5	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of physical security controls.
AT-3(8)	Role-based Training   Counterintelligence Training	Public sector enterprises should provide specialized counterinteligence awareness training that enables its resources to collect, interpret, and set upon a maje of data sources that may signat a foreign adversary's presence in the supply chain. At a minimum, counterinteligence training should cover known red flags, key information sharing concepts, and reporting requirements.	Functional	Intersects With	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection- related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
AT-3(8)	Role-based Training   Counterintelligence Training	Public sector enterprises should provide specialized counterinteligence awareness training that enables its resources to collect, interpret, and set upon a maje of data sources that may signat a foreign adversary's presence in the supply chain. At a minimum, counterinteligence training should cover known red flags, key information sharing concepts, and reporting requirements.	Functional	Equal	Counterintelligence Training	SAT-03.9	Mechanisms exist to provide specialized counterintelligence awareness training that enables personnel to collect, interpret and act upon a range of data sources that may signal the presence of a hostile actor.	10	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
AT-3(8)	Role-based Training   Counterintelligence Training	Public sector enterprises should provide specialized counterintelligence awareness training that enables its resources to collect, interpret, and set upon a maje of data sources that may signal a foreign adversary's presence in the upply chain. At a minimum, counterfinitelligence training should cover known red flags, key information sharing concepts, and reporting requirements.	Functional	Intersects With	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
AT-3(8)	Role-based Training   Counterintelligence Training	Public eachy enterprises should provide specialized counterintaligence experies training that enables its resources to collect, interprise, and act upon a range of data sources that may signal a flowing adversary's sees once in the supply data. As an arreporting requirements, and the standard should cover shown not flags, key information sharing concepts, and reporting requirements.	Functional	Intersects With	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
AT-4	Training Records	Enterprises should maintain documentation for C-SCRM-specific training, especially with regard to key personnel in acquisitions and counterintelligence.	Functional	Equal	Cybersecurity & Data Protection Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including basic cybersecurity and data protection awareness training, ongoing awareness training and specific-system training.	10	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 (Rasignment, organization-defined time period).
AU-1	Policy and Procedures	Enterprises must designate a specific official to manage the development, documentation, and dissemination of the until and accountability policy and procedures to include sudding of the supply chain information systems and network. The sudit 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, splars integrators, external systems service providers, and other ICT/ICT 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	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if alguitecant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	B. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:     Selection (one or more): Organization-level; Mission/Dusiness process-level; System-level] audit and accountability policy that:     Id Addresses burpose, scoope, roles.
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 solding of the supply chain information systems and network. The suidt and accountability policy and procedures should appropriately address tracking activities and their evaluability for other various supply chain activities, such as configura- datives tracking activities and their evaluability for other various supply chain activities, such as configura- magement. Suppliers, developers, system integrators, external system service providers and other ICDTOT- 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	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	Bevelop, document, and disseminate to [Assignment or oganization-defined personnel or roles]:     I [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that:     (a) Addresses purpose, scope, roles,
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 procedure to include auditing of the supply chain information systems and network. The audit and accountability policy and procedures should appropriately address ractings another installability for other various supply chain actively, such as configurably development. Suppliers, development, system integrations, setternal systems nervice providers, and other ICTOT- sections of the suppliers of the suppliers of the system integrations, and suppliers active suppliers of the sup	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	B. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:     Selection (one or more): Organization-level; Mission/husiness process-level; System-level] audit and accountability policy that:     (a) Addresses purpose, scoope, roles.
AU-2	Event Logging	An observable occurrence within the information system or supply chain network should be identified as a supply chain suitable event based on the enterprise's SDC context and requirements. Auditable events may include software/hardware changes, falled attempts to access supply chain information systems, or the movement of source ocks. Information on such events should be captured by speptrate sudiff mechanism and be traceable and verifiable. Information captured may include the type of event, datertime, length, and the fequency of courmers. Among other things, auditing may help detect missues of the supply chain the fequency of courmers. Among other things, auditing may help detect missues of the supply chain	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
AU-2	Event Logging	information systems or network caused by insister threats. Loss are a ker resource when identifying An observable occurrence within the information system or supply chain network should be identified as a supply chain auditable event based on the enterprise's SSLC context and requirements. Auditable event say include advant-entravene changes, falled attempts to access supply chain information systems, or the movement of source code. Information on such events should be captured by appropriate audit mechanisms and be traceable and verifiable. Information captured may include the type of event, datefuline, length, and the frequency of occurrence. Among other things, auditing may help eletect missue of the supply chain the frequency of occurrence. Among other things, auditing may help eletect missue of the supply chain	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	other organizational entities requiring audit- 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
AU-3	Content of Audit Records	Information systems or network caused by Inside Threats. Loss are a ker resource when identifying The earlit records of a supply chain event should be securely handled and maintained in a manner that operation to record retention requirements and preserves the integrity of the findings and the confidentiality of the record immation and its sources as appropriate. In certain instances, such records may be used in administrative or legisl proceedings. Enterprises should require their prime contractors to implement this continued and fined down this equipment for relevant sub-der contractors, prime contractors to implement this control and fined down this equipment for relevant sub-der contractors, prime contractors to implement their control and fined down this equipment to relevant sub-der contractors. Security of the contractors of the	Functional	Equal	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAS) to produce event logs that contain sufficient information to, at a minimum; (1) Establish what type of event occurred; (2) When (late and time) the event occurred; (3) When the event occurred; (3) When the event occurred; (3) When the event occurred; (4) When the event occurred; (5) When the event occurred; (6) When the event occurred; (7) When the event occurred; (8) When the event occurred; (9) When the event occurred; (9) When the event occurred; (1) When the event occurred; (1) When the event occurred; (1) When the event occurred; (1) When the event occurred; (2) When the event occurred; (3) When the event occurred; (4) When the event occurred; (5) When the event occurred; (6) When the event occurred; (7) When the event occurred; (8) When the event occurred; (8) When the event occurred; (8) When the event occurred; (9) When the event occur	10	other organizational entities requiring audit- fensure 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; e. Outcome of the event; a. Review and anayze system audit records
AU-6	Audit Record Review, Analysis, and Reporting	appropriately fiftered and correlated for enabyles 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 suddishe event, while an invalid signature is an information security auditable event. The combination of these two events may provide information valuable to CSGNM. The enterprise should adjust the level of sulf creor dreview based on the risk change leg. 4, excite threat interf. risk profile (on a specific yendor. Contracts should explicitly address how sudit findings will be reported and adjudicated.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	initial automatic book of unique a security involvent is term rainage (oters) or similar automatic book to support the centralized collection of security- related event logs.	5	(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-



ecure Controls Framework (SCF) 3 of 23

FDE#	FDE Name	Focal Document Element (FDE) Description NIST SP 800-161 R1 Supplemental C-SGRM Guidance	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		NIST SP 800-161 R1 Supplemental C-SCRM Guidance The enterprise should ensure that both supply chain and information security auditable events are	- rationale	netationship			Mechanisms exist to adjust the level of audit review, analysis and reporting	(ontional)	a. Review and analyze system audit records
AU-6	Audit Record Review, Analysis, and Reporting	appropriately filtered and consisted for analysis and reporting. For example, if new maintenance or a patch upgade is recognized to have an invalid eights alignature, the identification of the patch anviral 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 CSCRN. 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 windor. Contracts allowed societive address how audit findings with the record real additication.	Functional	Intersects With	Audit Level Adjustments	MON-02.6	based on evolving threat information from law enforcement, industry associations or other credible sources of threat intelligence.	5	[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-
AU-6(9)	Audit Record Review, Analysis, and Reporting   Correlation with Information from Nontechnical Sources	is a C-SCRM contact, non-technical sources include changes to the enterprise's security or operational policy, changes to the procurement or contracting processes, and notifications from suppliers, developers, system integrators, external systems enterly oproviders, and other ICT/OT-related service providers regarding plans to update, enhance, patch, or retire/dispose of a system/component.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non- technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization- wide situational awareness.	5	Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.
AU-10	Non-repudiation	Enterprises should implement non-repudiation techniques to protect the originality and integrity of both information systems and the supply chain network. Examples of what may require non-repudiation include supply chain metadata that describes the components, supply chain communication, and delivery acceptance information. For information systems, examples may include patch or maintenance upgrades for software as well as component replacements in a large hardware system. Verlying that such components originate from the OPH is part of non-repudiation.	Functional	Equal	Non-Repudiation	MON-09	Mechanisms exist to utilize a non-repudiation capability to protect against an individual falsely denying having performed a particular action.	10	Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [Assignment: organization-defined actions to be covered by non-repudiation].
AU-10(1)	Non-repudiation   Association of Identities	verifying that such components originate from the open is part or non-repolation.  This enhancement helps traceability in the supply chain and facilitates the accuracy of provenance.	Functional	Intersects With	Identity Binding	MON-09.1	Mechanisms exist to bind the identity of the information producer to the information generated.	5	(a) Bind the identity of the information producer with the information to [Assignment: organization defined strength of binding; and (b) Provide the means for authorized individuals to determine the identity of the producer of the information.
AU-10(2)	Non-repudiation   Validate Binding of Information Producer Identity	This enhancement validates the relationship of provenance and a component within the supply chain. Therefore, it ensures integrity of provenance.	Functional	Intersects With	Identity Binding	MON-09.1	Mechanisms exist to bind the identify of the information producer to the information generated.	5	(a) Validate the binding of the information producer identity to the information at [Assignment: organization-defined frequency]; and [OP Perform [Assignment: organization-defined actions] in the event of a validation error.
AU-10(3)	Non-repudiation   Chain of Custody	Chain of custody is fundamental to provenance and traceability in the supply chain. It also helps the verification of system and component integrity.	Functional	Intersects With	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5	Maintain reviewer or releaser credentials within the established chain of custody for information reviewed or released.
AU-12	Audit Record Generation	Enterprises should ensure that audit record generation mechanisms are in place to capture all relevant supply chain auditable events. Examples of such events include component version updates, component supply chain auditable events. Examples of such events include component version updates, component subserprises should require their prime contractors to implement this control and frow down this requirement to relevant sub-tier contractors. Departments and sigencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14202, Improving the Nation's Openeacity.	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
AU-13	Monitoring for Information Disclosure	Within the C-SCPM context, information disclosure may occur via multiple avenues, including open source information four perspective properties about derivation provided internation about an enterprise's system that increases the risk to that system. Enterprises should ensure that monitoring is in place for contractor systems to detect the unsurburised disclosure only data and that contract language includes a requirement that the vendor will notify the enterprise, in accordance with enterprise-defined time farmes and as soon as possible in the event of any potential or actual unantionized disclosure. Enterprises should require their prime in the event of any potential or actual unantionized disclosure.	Functional	Equal	Monitoring For Information Disclosure	MON-11	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of non-public information.	10	are to be logged by specific components of the a. Monitor [Assignment: organization-defined open-source information and/or information sites] [Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information; and b. If an information disclosure is discovered:
AU-14	Session Audit	contractors to implement this control and flow down this requirement to relevant sub-tier contractors.  Enterprises should include non-federal contract employees in session audits to identify security risks in the supply chain. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order  14028, Improving the Nation's Cybersecurity.	Functional	Equal	Session Audit	MON-12	Mechanisms exist to provide session audit capabilities that can: (1) Capture and log all content related to a user session; and (2) Remotely view all content related to an established user session in real time.	10	Notify IAssimment: organization-defined     Provide and implement the capability for     [Assignment: organization-defined users or roles]     to [Selection (one or more): record; view, hear;     log] the content of a user session under     [Assignment: organization-defined     circumstances]: and     b. Develoo. Integrate, and use session auditing
AU-16	Cross-organizational Audit Logging	In a C-SCRM context, this control includes the enterprise's use of system integrator or external service provider infrastructure. Enterprises should add language to contracts on coordinating audit information requirements and information exchange agreements with vendors.	Functional	Intersects With	Cross-Organizational Monitoring	MON-14	Mechanisms exist to coordinate santitzed event logs among external organizations to identify anomalous events when event logs are shared across organizational boundaries, without giving away sensitive or critical business data.	5	Employ [Assignment: organization-defined methods] for coordinating [Assignment: organization-defined audit information] among external organizations when audit information is transmitted across organizational boundaries.
AU-16(2)	Cross-organizational Audit Logging   Sharing of Audit Information	Whether managing a distributed audit environment or an audit databating environment between enterprises and it is system integrators or external services providers, enterprises should establish as soft requirements for the process of sharing audit information. In the case of the system integrator and external service provider and the enterprise, a service-level agreement of the type of audit data required versus what can be provided must be agreed to in a deviance to ensure that the enterprise of instain the relevant audit information needed to ensure that appropriate protections are in place to meet its mission operation protection resc. Ensure that coverage also that information sensors and supply chain strong are supported for the collection and	Functional	Equal	Sharing of Event Logs	MON-14.1	Mechanisms exist to share event logs with third-party organizations based on specific cross-organizational sharing agreements.	10	Provide cross-organizational audit information to [Assignment: organization-defined organizations] based on [Assignment: organization-defined cross-organizational sharing agreements].
CA-1	Policy and Procedures	Integrate the development and implementation of assessment and authorization policies and procedures for supply chain op/servoicin/ into the control assessment and authorization policy of related C-SCRM States/grimplementation Plank), policies, and system-level plans. To address opensecutiny risks throughout the supply chain, enterprises should develop a C-SCRM policy (or, if required, inflarges into outsiting 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 controlling control assessment and authorization, The C-SCRM role and responsibilities within the enterprise for controlling control assessment and authorization,	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection assessment and authorization controls.	10	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:     [Selection (one or more): Organization-level;     Mission/Dusiness process-level; System-level]     assessment, authorization, and monitoring
CA-1	Policy and Procedures	and decendencies among those roles, and the interaction among the roles. Entermise-wide security and 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 supply chain cybersecurity risks the control assessment and authorization policy and related C-SCRM 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 controling control assessment and authorization, the control assessment and submiration for the control assessment and submiration.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	nolizy that: 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] ssessement, authorization, and monitoring
CA-1	Policy and Procedures	any descendencies among those roles, and the interaction among the roles. Entermise-wide security and 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 supply chain 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.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybenecurity and data protection program, including policies, standards and procedures, at planned standards of significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	nolicy that: a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/Dusiness process-level; System-level] assessment, authorization, and monitoring
CA-2	Control Assessments	any dependencies among those roles, and the interaction among the roles, Enterorise-wide security and Ensure that the control assessment plan increportates releaved. CSCMM 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 baselines 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-relabel information. Enterprises abould verylen a startegy for collecting information, including a startegy for engaging with providers on supply chain risk assessments. Such collaboration helps enterprises learners information from providers and supply chain risk assessments. Such collaboration helps enterprises learners information from providers and learners and control a	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity and data protection policies and standards.	5	oblev that: 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
CA-2	Control Assessments	Inverse information from providers, reduce redundancy, identify obtaints courses of action for risk.  Exams that the control assessment plan incorporates relevant C-SOME controls and control enhancements.  The control assessment should cover the assessment of both information systems and the supply chain and aresure that an enterprise-relevant baselines set of controls and control enhancements are identified and used for the assessment. Control assessments are identified and used for the assessment. Control assessments are identified and used for the assessments. Control assessments can include information for morpolers quantity and active provider for control providers on supply chain risk sessements. Such collaboration letpe enterprises levents in from providers, enduce residuancy, definity potential courses of action for risk.	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (AP) activities to evaluate the design, implementation and effectiveness of technical cybersecurity and data protection controls.	5	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
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 useppl for the assessment. Control statessments can include information from supplier audits, reviews, and supply assessment of the second states, reviews, and supply states of the second states of the second states and the second states of t	Functional	Intersects With	Cybersecurity & Data Protection In Project Management	PRM-04	Mechanisms exist to assess cybersecurity and data protection 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
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 chains and ensure that an enterprise-relevant baseline set of controls and control enhancements are identified and usurply to the assessment. Control assessments can include information from supplier suits, reviews, and supply chain-relevant period of the property of the control assessments are including a stategy for collecting information, including a stategy for orgality with providers on supply chain inks sessments. Such collaboration helps enterprises	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity and data protection 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	Select the appropriate assessor or assessment team for the type of assessment to be conducted;     D. Develop a control assessment plan that describes the scope of the assessment including:     Controls and control enhancements under
CA-2	Control Assessments	Internate information from providers reduce redundancy, identify adoptinal courses of action for risk.  Exams that the control assessment plan incorporates relevant C-SORM controls and control enhancements.  The control assessment should cover the assessment of both information systems and the supply chain and aresure that an exteriorist-evierant baseline set of controls and control enhancements are identified and used for the assessment. Control assessments are identified and used for the assessment. Control assessments can include information from supplier audits, reviews, and supply chain resident information. Enterprises studied develop a strategy for collecting fromferation, including a strategy for engaging with providers on supply chain risk assessments. Such collaboration helps enterprises	Functional	Intersects With	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements.	5	Select the appropriate assessor or assessment to be conducted;     Develop a control assessment plan that describes the scope of the assessment including:
CA-2(2)	Control Assessments   Specialized Assessments	Internate information from movidiers, reduce resoundancy, identify, notential courses of action for risk.  Enterprises should use a variety of assessment techniques and methodologies, such as continuous movitoring, insider threat assessment, and malicious user assessment. These assessment mechanisms are content-apperfic and require the enterprise to undestant and its supply chain and to define the required set of measures for assessing and verifying that appropriate protections have been implemented.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for:  (1) Satutory, regulatory and contractual compliance obligations;  (2) Monitoring capabilities;  (3) Mobile devices;  (4) Otatabases;  (5) Application security;  (6) Application security;  (7) Application security;	5	Controls and control enhancements under include as part of control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced]. Selection (on or more): in-depth monitoring: security instrumentation; automated security test cases; vulnerability scanning; malicious user testing: insider threat assessment:
CA-2(3)	Control Assessments   Leveraging Results from External Organizations	For C-SCRM, enterprises should use external security assessments for suppliers, developers, system integrators, external system service providers, and other ICT/DTelated service providers. External sessessments include certifications, with party assessments, and — in the federal context — prior assessments performed by other departments and agencies. Certifications from the international Enterprises Standardization (Si). The National Information Assurance Partnership (Common Criteria), and the Open Group Trusted Technology Forum (OTTF) may also be used by non-federal and federal enterprises alike, if such certifications metal seneror needs.	Functional	Equal	Third-Party Assessments	IAO-02.3	this principlant heripotophose as $d$ in (11) after it.  Mechanisme solid to accept and respond to the results of external assessments that are performed by impartial, external organizations.	10	user testine: institer timest assessments, Leverage the results of control assessments performed by [Assignment: organization-defined external organization] on [Assignment: organization-defined system] when the assessment meets [Assignment: organization- defined requirements].



ecure Controls Framework (SCF) 4 of 23

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM	STRM	SCF Control	SCF#	Secure Controls Framework (SCF)	Strength of Relationship	Notes (optional)
100%	JOE Marile	NIST SP 800-161 R1 Supplemental C-SCRM Guidance The exchange of information or data between the system and other systems requires scrutiny from a supply	Rationale	Relationship	201 Controt	30/1	Control Description  Mechanisms exist to authorize connections from systems to other systems	/ontionall	a. Approve and manage the exchange of
CA-3	Information Exchange	chain perspective. This includes understanding the interface characteristics and connections of those components/systems that are directly interconnected or the data that is shared through those components/systems with developers, system integrators, external system service providers, other ICT/OT- related service providers, and — in some cases — suppliers. Proper servicetives agreements should be in place to ensure compliance to system information exchange requirements defined by the enterprise, as the transfer	Functional	Intersects With	System Interconnections	NET-05	using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection, the interface characteristics, cybersecurity and data protection requirements and the nature of the information communicated.	5	information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement;
		of information between systems in different security or privacy domains with different security or privacy.  For a system-level plan of actions and milestones (POA&Ms), enterprises need to ensure that a separate					Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or		service level agreements: user agreements:  a. Develop a plan of action and milestones for the
CA-5	Plan of Action and Milestones	PDASM exists for C-SCRM and includes both information systems and the supply chain. The C-SCRM PDASM should include tasks to be accomplished with a decommendation 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	Functional	Intersects With	Plan of Action & Milestones (POA&M)	IAO-05	similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	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;
CA-6	Authorization	externs or the supply chain any memdiation to address weatnesses, and any continuous monitorine Authorizing officials should include CSQMIn insultorisation decisions. To accomplish this, supply chain risks and compensating controls documented in CSGRM Plans or system security plans and the CSGRM PDABM should be included in the authorisation backage as part of the decision-misting process. Risks should be determined and associated compensating controls selected based on the output of criticality, threat, and underability analyses. Authorizing difficials may use the guidance in Section 2 of this document as well as	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	and  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;
CA-7	Continuous Monitoring	SISTIRE 179 to guide the assessment process.  For C-SCRM-specific guidance on this control, see Section 2 of this publication. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Operacurity.	Functional	Intersects With	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybensecurity and data protection controls oversight function that reports to the organization's executive leadership.	5	c. Ensure that the authorizing official for the system. before commencing operations: Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes: a. Establishing the following system-level metrics to be monitored: Rossimment:
CA-7(3)	Continuous Monitoring   Trend Analyses	The information gathered during continuous monitoring/trend analyses serves as input into C-SCRM decisions, including criticality analysis, vulnerability and threat analysis, and risk assessments, it also provides information that can be used in incident response and potentially identify a supply chain cybersecurity compress, including an insider theat.	Functional	Equal	Trend Analysis Reporting	MON-06.2	Mechanisms exist to employ trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.	10	restricts to the minimoleur, possigniment, organization-defined system-level metrics);  Employ tred analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.
CM-1	Policy and Procedures	Configuration management impacts nearly every aspect of the supply chain. Configuration management is critical to the enterprise's a billity to establish the provenance of components, including tracking and tracing them through the SOLC and the supply than. A properly defined and implemented configuration management capability provides greater assurance throughout the SDLC and the supply chain that components are authentic and have no been inappropriately condided. When defining a configuration	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	B. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/Dusiness process-level; System-level]
CM-1	Policy and Procedures	management policy and procedures, enterprises should address the full SDLC, including procedures for instruction and removing components to and from the enterprises information system boundary. A Configuration management imports nearly every aspect of the supply chain. Certifiquration management is criticated to the enterprise a faility to establish the provesance of components, lecturing tracking and tracing them through the SDLC and the supply chain. A properly defined and implemented configuration that the supply chain. A properly defined and implemented configuration components are sufficient to the components of the configuration management policy and procedures, enterprises should address the full SDLC, including procedures for introducing and removing components to and from the enterprises in formation supervise business.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing autability, adequacy and effectiveness.	5	configuration management policy that:  (a) Addresses pursones, scone, roles, a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/Dusiness process-level; System-level] configuration management policy that: (a) Addresses pursones, scone, roles.
CM-1	Policy and Procedures	Configuration management is abling to seally every aspect of the supply chain. Configuration management is activated to the entry of the supply chain. Configuration management is activated to the entry of the SDLC and the supply chain. A properly defined and implemented configuration than the supply chain and the supply chain 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	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	B. 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:
CM-2	Baseline Configuration	Introducine and removine components to and from the enterprise's information system boundary. A Enterprises should establish a baseline configuration of both the information system and the development environment, including documenting, formally reviewing, and securing the agreement of stakeholders. The purpose of the baseline is to provide a starting point for tracking changes to components, code, and/or settings throughout the SDLC. Regular reviews and updates of baseline configurations (i.e., re-baseling) are critical for traceability and provenance. The baseline configuration must take into consideration the enterprise's operational environment and any relevant supplies, developer, system integratior, external system	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 sc, or (3) As part of system component installations and upgrades.	5	(a) Addresses purpose, scope, roles, 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];
CM-2	Baseline Configuration	service covider, and other CTOT-related service provider involvement with the organization's information. Enterprises should establish a baseline configuration of both the information system and the development environment, including documenting, formally reviewing, and securing the agreement of stakeholders. The purpose of the baseline is to provide a starting point for tracking changes to components, code, and/or settings throughout the SIUC. 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 integration, external system service provider, and other CTOT-related service provider involvement with the operational formation service provider, and other CTOT-related service provider involvement with the operational formation service provider, and other CTOT-related service provider involvement with the operational formation service provider, and other CTOT-related service provider involvement with the operational formation service provider, and other CTOT-related service provider involvement with the operational formation and the provider of the component of the control of	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	When required due to IAssismment:     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:
CM-2(6)	Baseline Configuration   Development and Test Environments	The enterprise should maintain or require the maintenance of a baseline configuration of applicable suppliers, developers, system integration, external system service providers, and other ICT/OT-related service providers' development, test (and staging, if applicable) environments, and any configuration of interfaces.	Functional	Equal	Development & Test Environment Configurations	CFG-02.4	Mechanisms exist to manage baseline configurations for development and test environments separately from operational baseline configurations to minimize the risk of unintentional changes.	10	Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration.
CM-3	Configuration Change Control	Enterprises should determine, implement, monitor, and sudit configuration settings and change controls within the information systems and notworks and throughout the SDLC. This control supports traceability for C SCRM. The blown NIST SP 800-S3, Rev. 5 control enhancements – CM-3 (1), (2), (4), and (8) – are mechanisms that can be used for CSCRM to collect and manage change control data. Enterprises should require in prime contractors to implement this control and flow down this requirement to relevant sub-face contractors. Departments and agencies should refer the Appendix EV in primement this general in accordance with	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	Determine and document the types of changes to the system that are configuration-controlled;     Deview proposed configuration-controlled changes to the system and approve of disapprove such changes with explicit consideration for security and privacy impact
CM-3	Configuration Change Control	Executive Order 14028. Immorrant the Nation's Orbernscurity. Enterprises should determine, implement, monitor, and audit confliguration settings and change controls within the information systems and networks and throughout the SDLC. This control supports traceability for SDRN. The belown NITS F 900-SQ. Rev. Control enthancements—CN-s1(1), (2), (4), and (8) – are mechanisms that can be used for C-SCRM to collect and manage change control data. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-face contractors. Departments and agencies should refer to Appendix Fo implement this guidance in accordance with	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	analyses:  a. Determine and document the types of changes to the system that are configuration-controlled;  b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact
CM-3(1)	Configuration Change Control   Automated Documentation, Notification, and Prohibition of Changes	Executive Order 14028. Improving the Nation's Ordernsecurity.  Enterprises should define a set of system changes that are critical to the protection of the information system and the underlying or interoperating systems and networks. These changes may be defined assed on a criticality analysis (including components, processes, and functions) and where vulnerabilities exist that are not yet remediated e.g., due to resource constraints. The entage control process should also monitor for changes that may affect an existing security control to ensure that this control continues to function as required.	Functional	Equal	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization- approved change requests are received.	10	analyses: Use [Assignment: organization-defined automated mechanisms] to: (a) Document proposed changes to the system; (b) Notify [Assignment: organization-defined approval authorities] of proposed changes to the system and request change approval; (c) Hishlight proposed changes to the system
CM-3(2)	Configuration Change Control   Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing implementation of the changes.	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of cybersecurity and/or data privacy controls following implemented changes to ensure applicable controls operate as designed.	5	Test, validate, and document changes to the system before finalizing the implementation of the changes.
CM-3(2)	Configuration Change Control   Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing implementation of the changes.	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	5	Test, validate, and document changes to the system before finalizing the implementation of the changes.
CM-3(4)	Configuration Change Control   Security and Privacy Representatives	Require enterprise security and privacy representatives to be members of the configuration change control function.	Functional	Equal	Cybersecurity & Data Protection Representative for Asset Lifecycle Changes	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data privacy representative in the configuration change control review process.	10	Require [Assignment: organization-defined security and privacy representatives] to be members of the [Assignment: organization-defined configuration change control element].
CM-3(8)	Configuration Change Control   Prevent or Restrict Configuration Changes	Prevent or restrict changes to the configuration of the system under enterprise-defined circumstances.	Functional	Equal	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	10	Prevent or restrict changes to the configuration of the system under the following circumstances: [Assignment: organization-defined circumstances].
CM-4	Impact Analyses	Enterprises should take changes to the information system and underlying or interoperable systems and networks under consideration to determine whether the impact of these changes affects existing security controls and warman additional or different protection to maintain an acceptable level of cybensecurity 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-SCPM. NRT 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 sate servicement.	Functional	Equal	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	10	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.
CM-4(1)	Impact Analyses   Separate Test Environments	seatern from vulnerabilities that may be introduced through the test environment.  Analyze changes to the system in a separate test environment before implementing them into an operational environment, and look for securify and privacy impacts due to flaves, weaknesses, incompatibility, or intentional malice.	Functional	Equal	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unsuthroited access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	10	Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.
CM-5	Access Restrictions for Change	Enterprises should ensure that requirements regarding physical and logical access restrictions for changes to the information systems and networks are defined and included in the enterprise's implementation of access restrictions. Examples include access restriction for changes to centrally managed processes for software component updates and the deployment of updates or patches.	Functional	Intersects With	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to Technology Assets, Applications and/or Services (TAAS).	5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.



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 (optional)
							Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	Inntinnell	
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 'implementation of essential sections. Examples include access restriction for changes to entrally managed processes for software component updates and the deployment of updates or patches.	Functional	Intersects With	Access Restriction For Change	CHG-04		5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.
CM-5(1)	Access Restrictions for Change   Automated Access Enforcement and Audit Records	Enterprises should implement mechanisms to ensure automated access enforcement and auditing of the information system and the underlying systems and networks.	Functional	Equal	Automated Access Enforcement / Auditing	CHG-04.1	Mechanisms exist to perform after-the-fact reviews of configuration change logs to discover any unauthorized changes.	10	(a) Enforce access restrictions using [Assignment: organization-defined automated mechanisms]; and (b) Automatically generate audit records of the enforcement actions.
CM-5(6)	Access Restrictions for Change   Limit Library Privileges	Enterprises should note that software libraries may be considered configuration items, access to which should be managed and controlled.	Functional	Equal	Library Privileges	CHG-04.5	Mechanisms exist to restrict software library privileges to those individuals with a pertinent business need for access.	10	Limit privileges to change software resident within software libraries.
CM-6	Configuration Settings	Enterprises should oversee the function of modifying configuration settings for their information systems and networks and throughout the SDLC. Methods of oversight include periodic verification, reporting, and review, Resulting information may be shared with various parises that have access to, are connected to, or regige in the creation of the enterprise is 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 suddled to allerd designated enterprise personnel when a change has occurred. Enterprises should require their orime contractors to implement this configuration the relevant sub-tier their orime contractors to implement this configuration the relevant sub-tier.	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 (TAS) 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]:  h. Implement the configuration settings:
CM-6	Configuration Settings	Therepises should overtise the function of modifying configuration settings for their information systems and herepises should overtise the function of modifying configuration settings for their information systems and networks and throughout the SDC. Hethoid of oversight include periodic verification, reporting, and review, Resulting information may be shared with various parties that have access to, we connected to, or regige, in the creation of the enterprise is information systems and networks on a need-to-know basic. Danges should be tested and approve before they are implemented. Configuration settings should be monitored and sudded to alert designated enterprise personnel when a change has occurred. Enterprises should require their prime contractions to implement this configuration to religen should require their prime contractions to implement this configuration to relevant sub-tier	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	5	D. Implement use comparation settings as 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].  In Implement the configuration settings:
CM-6(1)	Configuration Settings   Automated Management, Application, and Verification	The enterprise should, when feasible, employ automated mechanisms to manage, apply, and verify configuration settings.	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	Manage, appty, and verify configuration settings for [Assignment: organization-defined system components] using [Assignment: organization-defined automated mechanisms].
CM-6(2)	Configuration Settings   Respond to Unauthorized Changes	The enterprise should ensure that designated security of IT personnel are alerted to unauthroited changes to configuration settling. When suppliers, evenlopers, system integrators, external system service providers, and other ICI/OT-related service providers are responsible for such unauthroited changes, this qualifies as a C-SCRM incident that should be recorded and tracked to monitor tends. For a more complemense view, a specific, predefined set of C-SCRM stakeholders should assess the impact of unauthroited changes in the supply chain. When impact is sessessed, relevant stakeholders should help define and implement accorocities implication strategies to the sessessed relevant stakeholders should help define and implement accordistic implication strategies to	Functional	Equal	Respond To Unauthorized Changes	CFG-02.8	Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents.	10	Take the following actions in response to unauthorized changes to [Assignment: organization-defined configuration settings]: [Assignment: organization-defined actions].
CM-7	Least Functionality	assessed, relevant stakeholders should help define and implement appropriate mitration statedies to Least functionally induces the states usine. Enterprises should ensure least functionally in the inability to specify and implement least functionality. Enterprises should ensure least functionality in their information systems and networks and throughout the SDLC. NSTS 98 looks, 8.e., 5 control enterprises and systems and several some states of the state of the states of	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.
CM-7(1)	Least Functionality   Periodic Review	Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Equal	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	10	(a) Review the system [Assignment: organization- defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and (b) Disable or remove [Assignment: organization- defined functions, ports, protocols, software, and services within the system deemed to be
CM-7(4)	Least Functionality   Unauthorized Software — Deny-by-exception	Enterprises should define requirements and deploy appropriate processes to specify and detect software that is not allowed. This can be aided by defining a requirement to, at a minimum, not use disreputable or unauthorized software. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors	Functional	Equal	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	10	(a) Identify [Assignment: organization-defined software programs not authorized to execute on the system]; (b) Employ an allow-silt, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; and (c) Review and update the list of unauthorized
CM-7(5)	Least Functionality   Authorized Software — Allow-by-exception	Enterprises should define requirements and deploy appropriate processes to specify allowable software. This can be added by defining a requirement to use only reputable software. This can also include requirements for a	Functional	Equal	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowfist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	10	(a) Identify (Assignment: organization-defined software programs authorized to execute on the system); (b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and (c) Review and update the list of authorized
CM-7(6)	Least Functionality   Confined Environments with Limited Privileges	The enterprise should ensure that code authentication mechanisms such as digital signatures are implemented when executing code to assure the integrity of software, firmware, and information on the information systems and networks.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	Require that the following user-installed software execute in a confined physical or virtual machine environment with limited privileges: [Assignment: organization-defined user-installed software].
CM-7(7)	Least Functionality   Code Execution in Protected Environments	The enterprise should obtain binary or machine-executable code directly from the OEM/developer or other acceptable, verified source.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	Allow execution of binary or machine-executable code only in confined physical or virtual machine environments and with the explicit approval of (Assignment: organization-defined personnel or roles) when such code is:  (a) Obtained from sources with limited or no
CM-7(8)	Least Functionality   Binary or Machine Executable Code	When exceptions are made to use software products without accompanying source code and with limited or no warranty because of competiting mission or operational requirements, approval by the authorizing difficial should be contingent upon the enterprise expectifily incorporating cybersecurity supply chain risk assessments as part of a broader assessment of such software products, as well as the implementation of compensating control to address any inferrited and assessed risks.	Functional	Equal	Binary or Machine- Executable Code	END-06.7	Mechanisms exist to prohibit the use of binary or machine-executable code from sources with limited or no warranty and without access to source code.	10	warranty: and/or (a) Prohibit the use of binary or machine- executable code from sources with limited or no warranty or without the provision of source code; and (b) Allow exceptions only for compelling mission or operational requirements and with the
CM-7(9)	Least Functionality   Prohibiting The Use of Unauthorized Hardware	Enterprises should define requirements and deploy appropriate processes to specify and detect handware that is not allowed. This can be aided by defining a requirement to, at a minimum, not use disreputable or usuallocide than the Enterprises should require their prime contractors to implement this control and flow down this equirement to referent use the control can.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	sooroval of the authorizina official.  (a) identify [Assignment: organization-defined hardware components authorized for system use];  (b) Prohibit the use or connection of unauthorized hardware components;  (c) Review and update the list of authorized
CM-8	System Component Inventory	Enterprises should ensure that critical component assets within the information systems and networks are included in the asset inventory. The inversory must also include information for critical component accountability, inventory information includes, for example, hardware inventory specifications, software social markets, owhere version inventors, component owners, and for networked components or devices — machine names and network addresses, inventory specifications may include the manufacture, device by personal central number, and oplysical location. Enterprises should require their prime contractors device by personal central number, and oplysical location. Enterprises should require their prime contractors	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	5	hardware components fassiemment organization- 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;
CM-8	System Component Inventory	to implement this control and flow down this requirement to relevant author controlers. Enterprises should Enterprises should are nave that critical component assets within the information systems and networks are included in the asset inventory. The inventory must also include information for critical component accountability, inventory information includes, for example, hardware inventory specifications, software iscense information, software vestion numbers, component owners, and for networked components or devices—muchine names and network discesses. Inventory specifications may include the manufacturer, deviced type, model, serial number, and physical location. Emerphises should require their prime contractors	Functional	Intersects With	Component Duplication Avoidance	AST-02.3	Insortins:  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	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
CM-8(1)	System Component Inventory   Updates During Installation and Removal	to implement this control and flow down this requirement to relevant subtles contractors. Enterorises should  When installing, updating, or removing an information system, information system component, or network component, the enterprise needs to update the inventory to ensure trace-billing for tracking chifical components. In addition, the information system's configuration needs to be updated to ensure an accurate inventory of supply chain protections and then re-baselined accordingly.	Functional	Equal	Updates During Installations / Removals	AST-02.1	Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.	10	other system:  Update the inventory of system components as part of component installations, removals, and system updates.
CM-8(2)	System Component Inventory   Automated Maintenance	The enterprise should implement automated maintenance mechanisms to ensure that changes to component inventory for the information systems and networks are monitored for installation, update, and removal. When automated maintenance is performed with a predefined frequency and with the automated collation of relevant inventory information about each defined component, the enterprise should ensure that updates are available to relevant stakeholders for evaluation. Predefined frequencies for data collection should be less predictable in order to reduce the risk of an insider threat bysassing security mechanisms.	Functional	Equal	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	10	Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms].
CM-8(4)	System Component Inventory   Accountability Information	The enterprise should ensure that accountability information is collected for information system and network components. The systemic component inventory information should identify those individuals who originate an acqualition as well as intended and users, including any associated personnel who may administer or use the system/components.	Functional	Equal	Accountability Information	AST-03.1	Mechanisms exist to include capturing the name, position and/or role of includiduals responsible/accountable for administering assets as part of the technology asset inventory process.	10	Include in the system component inventory information, a means for identifying by [Selection (one or more): name; position; role]. Individuals responsible and accountable for administering those components.
CM-8(6)	System Component Inventory   Assessed Configurations and Approved Deviations	Assessed configurations and approved deviations must be documented and tracked. Any changes to the baseline configurations of information systems and networks require a review by relevant stakeholders to ensure that the changes do not result in increased exposure to cybersecurity risks throughout the supply chain.	Functional	Equal	Approved Baseline Deviations	AST-02.4	Mechanisms exist to document and govern instances of approved deviations from established baseline configurations.	10	Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM	STRM	SCF Control	SCF#	Secure Controls Framework (SCF)	Strength of	Notes (optional)
102#	7 DE Name	NIST SP 800-161 R1 Supplemental C-SCRM Guidance Enterprises may choose to implement centralized inventories that include components from all enterprise	Rationale	Relationship	oor control	501.0	Control Description  Mechanisms exist to implement and manage a Configuration Management	/ontionall	Notes (apriority)
CM-8(7)	System Component Inventory   Centralized Repository	information systems, networks, and their components. Centralized repositories of inventories provide opportunities for delicinacies in accounting for information systems, networks, and their components. Such repositories may also help enterprises rapidly identify the location and responsible individuals of components that have been componented, breached, or are otherwise in need of militigation sciencis. The enterprise ehould ensure that centralized inventories include the supply chain-specific information required for proper components accountable bits. As supply chain relevance and information systems reviews, or concovent components accountable bits.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.  Mechanisms exist to track the geographic location of system components.	5	Provide a centralized repository for the inventory of system components.
CM-8(8)	System Component Inventory   Automated Location Tracking	When employing automated mechanisms for tracking information system components by physical location, the enterprise should incorporate information system, network, and component tracking needs to ensure accurate inventory	Functional	Equal	Automated Location Tracking	AST-02.10		10	Support the tracking of system components by geographic location using [Assignment: organization-defined automated mechanisms].
CM-8(9)	System Component Inventory   Assignment of Components to Systems	When assigning components to systems, the enterprise should ensure that the information systems and networks with all relevant components are inventioned, marked, and properly assigned. This isolatates quick inventory and accomponents relevant to information systems and retevorks and enterbests tracking of components that are considered critical and require differentiating treatment and part of the information systems and relevant protection achieving systems and relevant protection achieving.	Functional	Equal	Component Assignment	AST-02.11	Mechanisms exist to bind components to a specific system.	10	(a) Assign system components to a system; and (b) Receive an acknowledgement from [Assignment: organization-defined personnel or roles] of this assignment.
CM-8(10)	System Component Inventory   SBOMs for Open Source Projects	If an enterprise uses an open source project that does not have an SBOM and the enterprise requires one, the enterprise will need to 1) contribute SBOM generation to the open source project, 2) contribute resources to the project to add this capability, or 3) generate an SBOM on their first consumption of each version of the open source project that they use.	Functional	Intersects With	Open Source Software	CFG-04.1	Mechanisms exist to establish parameters for the secure use of open source software.	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
CM-8(10)	System Component Inventory   SBOMs for Open Source Projects	If an enterprise uses an open source project that does not have an SBOM and the enterprise requires one, the enterprise will need to 1) contribute SBOM generation to the open source project, 2) contribute resources to the project to add this capability, or 3) generate an SBOM on their first consumption of each version of the open source project that they use.	Functional	Intersects With	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative Assembled to the Configurati	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
CM-8(10)	System Component Inventory   SBOMs for Open Source Projects	If an enterprise uses an open source project that does not have an SBOM and the enterprise requires one, the enterprise will need to 1) contribute SBOM generation to the open source project, 2) contribute resources to the project to add this capability, or 3) generate an SBOM on their first consumption of each version of the open source project that they use.	Functional	Intersects With	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security controls to be utilized within Technology Assets, Applications and/or Services (TAAS) in sufficient detail to permit analysis and testing of the controls.	5	This specific NIST 800-161 R1 control does not exist in MIST 800-53 R5.
CM-8(10)	System Component Inventory   SBOMs for Open Source Projects	If an enterprise uses an open source project that does not have an SBOM and the enterprise requires one, the enterprise will need to 1) contribute SBOM generation to the open source project. 2 contribute resources to the project to add this capability, or 3) generate an SBOM on their first consumption of each version of the open source project that they use.	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate, or obtain, a Software Bill of Materials (ISBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	5	This specific NIST 800-161 R1 control does not exist in MIST 800-53 R5.
CM-8(10)	System Component Inventory   SBOMs for Open Source Projects	Ean enterprise uses an open source project that does not have an SBOM and the enterprise requires one, the enterprise will need to 1) contribute SBOM generation to the open source project, 2) contribute resource to the project to add this capability, or 3) generate an SBOM on their first consumption of each version of the open source project that they use.	Functional	Intersects With	Developer Architecture & Design	TDA-05	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAS) to produce a design specification and security achievite that: (1) is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; (2) Acquirated word commission for the 1/2 Acquiration with commission for activities that remained securities functionality.	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
CM-9	Configuration Management Plan	Enterprises should ensure that C-SCRM is incorporated into configuration management planning activities. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Subset Of	Configuration Management Program	CFG-01	If a continuous and reference to the implementation of configuration management controls.	10	Develop, document, and implement a configuration management plan for the system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying
CM-9	Configuration Management Plan	Enterprises should ensure that C-SCRM is incorporated into configuration management planning activities. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5	Design, document, and implement a configuration management plan for the system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying
CM-9(1)	Configuration Management Plan   Assignment of Responsibility	Enterprises should ensure that all relevant roles are defined to address configuration management activities for information systems and networks. Enterprises should ensure that requirements and capabilities for configuration management are appropriately addressed or included in the following supply chain activities: requirement solinition, development, estign, market research and analysis, procurement solicitations and contracts, component installation or removal, system integration, operations, and mainternance.	Functional	Equal	Assignment of Responsibility	CFG-01.1	Mechanisms exist to implement a segregation of duties for configuration management that prevents developers from performing production configuration management duties.	10	Assign responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.
CM-10	Software Usage Restrictions	Enterprises should ensure that licenses for software used within their information systems and networks are documented, tracked, and maintained. Tracking mechanisms should provide for the ability to trace users and the use of licenses to access control information and processes. As an example, when an employee is terminated, a "named user licenses should be revoked, and the license documentation should be updated to reflect this change. Departments and agencies should refler to Appendix for implement this guidance in accordance with Executive Order 1402s, improving the Nation's Oplersecutive.	Functional	Equal	Software Usage Restrictions	CFG-04	Mechanisms exist to enforce software usage restrictions to comply with applicable contract agreements and copyright laws.	10	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     Control and document the use of peer-to-peer
CM-10(1)	Software Usage Restrictions   Open- source Software	When considering software, enterprises should review all options and corresponding risks, including open source or commercially licensed components. When using open source software (DSS), the enterprise should understand and review the open source confirmed to the control of the control o	Functional	Equal	Open Source Software	CFG-04.1	Mechanisms exist to establish parameters for the secure use of open source software.	10	Establish the following restrictions on the use of open-source software: [Assignment: organization- defined restrictions].
CM-11	User-installed Software	This control extends to the enterprise information system and network users who are not employed by the enterprise. These users may be supplien, developers, system integrators, external system service providers, and other ICI/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
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 supplien, 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	e. Monitor ooliv compliance IAssisment. a. Establish IAssignment: organization-defined policies) governing the installation of software by users; b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; and
CM-12	Information Location	Information that resides in different physical locations may be subject to different cybensecurity risks throughout the supply chain, depending on the specific location of the information. Components that originate or operate from different physical locations may also be subject to different supply chain risks, depending on the specific location of origination or operations. Enterprises should manage these risks through limiting access control and specifying allowable of disallowable segosphic locations for backup/recovery, patching/upgrades, and information transfer/sharing, NRT SP 800-53, Rev. 5 control enhancement CM-12 (1) is a mechanism that can be used to enable automated location of components.	Functional	Equal	Information Location	DCH-24	Mechanisms exist to identify and document the location of information and the specific system components on which the information resides.	10	e. Monitor oolivo comoliance (Assiament. a. Identify and document the location of (Assignment: organization-defined information) and the specific system components on which the information is processed and stored: b. Identify and document the users who have access to the system and system components
CM-12(1)	Information Location   Automated Tools to Support Information Location	is a mechanism that can be used to ensible automated location of components.  Use automated tools to identify enterprise-defined information on enterprise-defined system components to ensure that controls are in place to protect enterprise information and individual privacy.	Functional	Equal	Automated Tools to Support Information Location	DCH-24.1	Automated mechanisms exist to identify by data classification type to ensure adequate cybersecurity and data protection controls are in place to protect organizational information and individual data privacy.	10	where the information is processed and stored; Use automated tools to identify (Assignment: organization-defined information by information type) on (Assignment: organization-defined system components) to ensure controls are in place to protect organizational information and individual privacy.
CM-13	Data Action Mapping	in addition to personally identifiable information, understanding and documenting a map of system data actions for sensitive or classified information is necessary. Data action mapping should also be conducted to map interent of Things [30] devices, entroded or stand-alone to Fystems, or of system of system data actions. Understanding what classified or for information is being processed, its sensitivity and/or effect on a physical thing or physical environment. Now the sensitive or of information is being processed (e.g., if the data action is visible to an individual or is processed in another part of the system), and by whom provides a number of contenting factors that are minorant for cassessing the degree of its. Other areas can be illustrated	Functional	Equal	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of technology assets where sensitive/regulated data is stored, transmitted or processed.	10	Develop and document a map of system data actions.
CM-14	Signed Components	Enterprises should verify that the acquired hardware and software components are genuine and valid by using digitally signed components from trusted certificate authorities. Verifying components before allowing installation helps enterprises reduce cybersecurity risks throughout the supply chain.	Functional	Intersects With	Signed Components	CHG-04.2	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.	5	Prevent the installation of [Assignment: organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that it recognized and approved by the organization.
CP-1	Policy and Procedures	Enterprises should integrate C-SCRM into the contingency planning policy and related SCRM Strategy/implementation Plan, policies, and SCRM Plan. The policy should over information systems and the supply than network and, at a minimum, address scenarios such as: a. Unplanned component failure and subsequent replacement; b. Planned replacement related to feature improvements, maintenance, upgrades, and modernization; and c. Product and/or service disruption.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, sandards and procedures, at planned intervals or it 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: [as Addresses ourroses, scoop, roles.
CP-1	Policy and Procedures	Enterprises should integrate C-SCRM into the contingency planning policy and related SCRM States/grimplementation 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. Inplanned component failure and subsequent replacement; b. Planned replacement traislet of betause 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 enure resilient Technique Saesta, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/OR) playbooks).	10	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:     [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that:     [a] Addresses purpose, scope, roles,



		Focal Document Element (FDE) Description	STRM	STRM			Secure Controls Framework (SCF)	Strength of	
FDE#	FDE Name	NIST SP 800-161 R1 Supplemental C-SCRM Guidance	Rationale	Relationship	SCF Control	SCF#	Control Description  Mechanisms exist to establish, maintain and disseminate cybersecurity	Relationship	Notes (optional)  a. Develop, document, and disseminate to
CP-1	Policy and Procedures	Enterprises should integrate C-SCRN into the contingency planning policy and related SCRN Strategylimplementation Plant, policies, and SCRNP lins. The policy should cover information systems and the supply chain network and, at a minimum, address scenarios such as: a. Unplanned component fallule and subsequent replacement; b. Planned replacement related to feature improvements, maintenance, upgrades, and modernization; and c. Product and/or service disrupption.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Prechamans axis to establish, maintain and disseminate cyclerisecurity and data protection policies, standards and procedures.	5	a. Develop, ubcunient, and ubsammate 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, scoope, roles.
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 degadation of data or operations. Contrigencies should be put in place for the supply chain, relower, information systems (sepecially 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:
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, revolven, information systems (sepecially critical components), and processes to ensure protection against compromise and provide appropriate failover and firmly 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., personnet 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	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:
CP-2(1)	Contingency Plan   Coordinate with Related Plans	Coordinate contingency plan development for supply chain risks with enterprise elements responsible for related plans.	Functional	Equal	Coordinate with Related Plans	BCD-01.1	(6) Eartilities to # new attend or decommissioned obtained Mechanisms soits to coordinate configency plan development with internal and external elements responsible for related plans.	10	Coordinate contingency plan development with organizational elements responsible for related plans.
CP-2(2)	Contingency Plan   Capacity Planning	This enhancement helps the availability of the supply chain network or information system components	Functional	Equal	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	10	Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.
CP-2(7)	Contingency Plan   Coordinate with External Service Providers	Enterprises should ensure that the supply chain network, information systems, and components provided by an external service provider have appropriate failurer to include personnel, equipment, and network resources) to recolor or prevent service interruption or ensure interly ecoverys, Enterprises should ensure that contingency planning requirements are defined as part of the service-level agreement. The agreement may have specific terms that address critical components and functionally support in case of denial-of-service stacks to ensure the continuity of operations. Enterprises should coordinate with external service providers to identify service ovoliders "distint continuers valar practices and build on them as required by the continuity of the providers "distint continuers valar practices and build on them as required by the continuity."	Functional	Equal	Coordinate With External Service Providers	BCD-01.2	Mechanisms exist to coordinate internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.	10	Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.
CP-2(8)	Contingency Plan   Identify Critical Assets	Ensure that critical assets (including hardware, software, and personnel) are identified and that appropriate contingency planning requirements are defined and applied to ensure the continuity of operations. A key step in this process is to complete a criticality analysis on components, functions, and processes to identify all critical assets. See Section 2 and NISTIR 8179 for additional guidance on criticality analyses.	Functional	Equal	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TASD) that support essential missions and business functions.	10	Identify critical system assets supporting [Selection: all; essential] mission and business functions.
CP-3	Contingency Training	Enterprises should ensure that critical suppliers are included in contingency training. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies bould refer to Appendix for 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	<ul> <li>a. Provide contingency training to system users consistent with assigned roles and responsibilities:</li> <li>1. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility:</li> <li>2. When required by system chanses: and</li> </ul>
CP-3(1)	Contingency Training   Simulated Events	Enterprises should ensure that suppliers, developers, system integration, external system service providers, and other ICT/OT-resisted service providers who have roles and responsibilities in providing critical services are included in contingency training eventiess.	Functional	Equal	Simulated Events	BCD-03.1	Mechanisms exist to incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.	10	Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.
CP-4	Contingency Plan Testing	Enterprises should ensure that critical suppliers are included in contingency testing. The enterprise – in coordination with the service provider(s) – should test continuity/testilency capabilities, such as failover from a primary production site to a back-up oak. 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 Ptan Root Cause Analysis (RCA) & Lessons Leamed	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 plant [Assignment: organization- defined tests]. b. Review the contingency plan test results; 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 one. This testing may coordinate to 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 confingency 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 reactiness to execute the plan: [Assignment: organization- defined tests]. b. Review the contineency olan test results: and
CP-6	Alternate Storage Site	When managed by suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, alternative storage sites are considered within an enterprise's supply chain network. Enterprises should apply appropriate cybersecurity supply chain controls to those storage sites.	Functional	Equal	Alternate Storage Site	BCD-08	Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information.	10	a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.
CP-6(1)	Alternate Storage Site   Separation from Primary Site	This enhancement helps the resiliency of the supply chain network, information systems, and information system components.	Functional	Equal	Separation from Primary Site	BCD-08.1	Mechanisms exist to separate the alternate storage site from the primary storage site to reduce susceptibility to similar threats.	10	Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.
CP-7		When managed by suppliers, developers, system integrators, external system service providers, and other ICT/GT-related service providers, alternative storage sites are considered within an enterprise's supply chain. Enterprises should apply appropriate supply chain cybersecurity controls to those processing sites.	Functional	Equal	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides securify measures equivalent to that of the primary site.	10	a. Establish an attenate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point
CP-8	Telecommunications Services	Enterprises should incorporate atternative telecommunication service providers for their supply chain to support critical information systems.	Functional	Intersects With	Telecommunications Services Availability	BCD-10	Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.	5	Establish afternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications.
CP-8(3)	Telecommunications Services   Separation of Primary and Alternate Providers	The separation of primary and alternative providers supports cybersecurity resilience of the supply chain.	Functional	Equal	Separation of Primary / Alternate Providers	BCD-10.2	Mechanisms exist to obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.	10	Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.
CP-8(4)	Telecommunications Services   Provider Contingency Plan	For C-SCRM, suppliers, developers, system integrators, external system service providers, and other ICT/OT- related service providers, contingency plans should provide separation in infrastructure, service, process, and personnel, where appropriate.	Functional	Equal	Provider Contingency Plan	BCD-10.3	Mechanisms exist to contractually-require external service providers to have contingency plans that meet organizational contingency requirements.	10	(a) Require primary and atternate telecommunications service providers to have contingency plans; (b) Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and
CP-11	Alternate Communications Protocols	Enterprises should ensure that critical suppliers are included in contingency plans, training, and testing as part of incorporating alternative communications protocol capabilities to establish supply chain resilience.	Functional	Intersects With	Telecommunications Services Availability	BCD-10	Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.	5	Provide the capability to employ [Assignment: organization-defined atternative communications protocola] in support of maintaining continuity of operations.
IA-1	Policy and Procedures	The enterprise should – at enterprise-defined intervals – review, enhance, and update their identify and access management policies and procedures to ensure that critical roles and processes within the supply chain restored are defined and that the enterprise s-critical systems, components, and processes are identified for trace-boility. 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 of all terms within the supply chain would be cost-prohibitive, and discretion should be used. The enterprise should under related C-SOR Strates/relimementation Planish   Dockles, and C-SCRPM Instrumentation Planish   Dockles, and C-SCRPM	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, sundands and procedures, at planned internals or it 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.
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 terms within the supply chain would be cost-prohibitive, and discretion should be used. The enterprise should under related C-SOR Strateer/windementation Planiah. Divide; and C-SORP Microse.	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/Dusiness process-level; System-level] identification and authentication policy that: [c] Middlessers purpose sponse of persons.
IA-1	Policy and Procedures	The enterprise should—at enterprise-defined inferensis—review, enhance, and update their identify and saccess management policies and procedures to ensure that critical releas and processes within the supply chain network are defined and that the enterprise's critical systems, components, and processes are sentified for traceability. This should include the identify of critical components that may not have been considered under identification and suthertication in the past. Note that providing identification for all times within the supply chain would be cost-positibility, and discinction should be used. The enterprise should used are related C-SCRM Strateavimolementation Planisis. Policies and C-SCRM Plans.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	Bevellop, document, and disseminate to [Assignment: organization-defined personnel or rotes]:  1 [Selection (one or more): Organization-level; Hissien/business process-level; System-level] identification and authentication policy that:  (a) Addresses purpose, scope, rotes.



ecure Controls Framework (SCF) 8 of

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 (optional)
		Enterprises should ensure that identification and requirements are defined and applied for enterprise users accessing an ICT/OT system or supply chain network. An enterprise user may include employees, individuals					Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on	innlinnell	
IA-2	Identification and Authentication (organizational Users)	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	Functional	Equal	Identification & Authentication for Organizational Users	IAC-02	behalf of organizational users.	10	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.
IA-3	Device Identification and Authentication	inclement this control and flow down this requirement to relevant sub-lief contractors. Departments and Enterprises should implement capabilities to distinctly and positively identify devices and software within their supply chain and, once identified, verify that the identify is authentic. Devices that require unique device to device identification and substratication should be defined by type, device, or a combination of type and device. Software that requires authentification should be identified through a software identification tag (SWIO) that enables verification of the software package and authentication of the enterprise releasing the software package.	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically-based and replay resistant.	5	Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.
IA-4	Identifier Management	Ventifiers allow for greater discoverability and traceability. Within the enterprise's supply chain, identifiers should be assigned to systems, individuals, documentation, devices, and components. In some cases, identifiers may be maintained throughout a system's life cycle—from concept to retirement – but, at a minimum, throughout the system's life within the enterprise.  For software development, identifiers should be assigned for those components that have achieved	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	Manage system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier; b. Selecting an identifier that identifies an
IA-4	Identifier Management	configuration item recognition. For devices and operational visitems, identifiers should be assigned when the Mertifiers allow for greater discoversality and traceability, with the enterprise is supply chain, ilentifiers should be assigned to systems, individuals, documentation, devices, and components. In some cases, identifiers may be entainstead throughout a system's life cylind—from concept to retirement—but, at a minimum, throughout the system's life within the enterprise. For software development, identifiers should be assigned for those components that have achieved configuration item recontinion. For devices and operations it stems, identifiers alloud be assigned when the	Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usemames and Technology Assets, Applications and/or Services (TAAS).	5	individual, group, role, service, or device:  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:
IA-4(6)	Identifier Management   Cross-organization Management	This enhancement helps the traceability and provenance of elements within the supply chain through the coordination of dentifier management among the enterprise and its suppliers, developers, system integrations, determine yellower sometime forwards and other forth-oriented service quotiests. This includes information systems and components as well as individuals engaged in supply chain activities.	Functional	Equal	Cross-Organization Management	IAC-09.4	Mechanisms exist to coordinate username identifiers with external organizations for cross-organization management of identifiers.	10	Coordinate with the following external organizations for cross-organization management of identifiers: [Assignment: organization-defined external organizations].
IA-5	Authenticator Management	This control facilitates traceability and non-repudiation throughout the supply chain. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecurity	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage autherticators for users and devices; and (2) Ensure the straign of authertication 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:
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. Verliying, a 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:
IA-5(5)	Authenticator Management   Change Authenticators Prior to Delivery	This enhancement verifies the chain of custody within the enterprise's supply chain.	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.
IA-5(9)	Authenticator Management   Federated Credential Management	This enhancement facilitates provenance and chain of custody within the enterprise's supply chain.	Functional	Equal	Federated Credential Management	IAC-13.2	Mechanisms exist to federate credentials to allow cross-organization authentication of individuals and devices.	10	Use the following external organizations to federate credentials: [Assignment: organization-defined external organizations].
IA-8	Identification and Authentication (non- organizational Users)	Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers have the potential to engage the enterprise's supply chain for service delivery (e.g., development/lingsation services, product support, etc.). Enterprise should manage the establishment, sauditing, use, and revocation of identification credentials and the authentication of non-enterprise users within the supply chain. Enterprises should also ensure prompterss in performing identification and suthentication activities, especially in the case of revocation management, to help mitigate exposure to cyclemecurity risks throughout the supply chain such as those that since due to inside threats.	Functional	Equal	Identification & Authentication for Non- Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	10	Uniquely identify and authenticate non- organizational users or processes acting on behalf of non-organizational users.
IA-9	Service Identification and Authentication	Therefore is not uncounted that control and submitted that a such as the submitted that are such as some states and the submitted that are defined and makinged for access to service to e.g., who applications using digital certificate, services or applications that query a database as opposed to labor services) throughout the supply chain. Enterprise should ensure that they know when services are being procured and from whom. Services procured should be listed on a validated list of services to the enterprise or have compensating control in place. Enterprise should require their prime contractors to implement this control and flow down this requirement to relevant sub-less control care.	Functional	Equal	Identification & Authentication for Third- Party Assets, Applications & Services	IAC-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).	10	Uniquely identify and authenticate [Assignment: organization-defined system services and applications] before establishing communications with devices, users, or other services or applications.
IR-1	Policy and Procedures	Enterprises should integrate C-SCRM into incident response policy and pocedures, and related C-SCRM Strategy/implementation Plans and Policies. The policy and procedures must provide direction for how to address supply chain-related incidents and cybersecurity incidents that may complicate or impact the supply chain. Individuals who work within specific mission and system environments need to recognize cybersecurity supply chain-related incidents. The incident response policy should state when and how threats and incidents should be handled, reported, and managed.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	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, scoop, roles,
IR-1	Policy and Procedures	Enterprises should integrate C-SCRM into incident response policy and posedures, and related C-SCRM Statesgl/mighementation Plans and Policies. The policy and procedures must provide direction for how to address supply chain-related incidents and cybersocurity incidents that may complicate or impact the supply chain. Incidental services with specific mission and system supply chain incidental who work within specific mission and system environments need to recognize cybersocurity supply chain-related incidents. The incident response policy strought states when and how threats and incidents should be farefacely, reported, and managed.	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	Develop, document, and disseminate to [Assignment: organization-defined personnel or rotes]:     [Selection (one or more): Organization-tevel; Mission/Dusiness process-level; System-level] incident response policy that:     [Aldriesses purpose, score, roles,
IR-1	Policy and Procedures	Enterprises should integrate C-SCRN into incident response policy and poscedures, and related C-SCRN Statesgy/mighemetration Plans and Policies. The policy and procedures must provide direction for how to saddress supply chain-related incidents and cybersecurity incidents that may complicate or impact the supply chain, incidents who work within specific mission and system environments need to recognize cybersecurity supply chain-related incidents. The incident response policy should state when and how threats and incidents should be handled, reported, and managed.	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate tessons learned, business process changes and industry developments, as necessary.	5	Develop, document, and disseminate to [Assignment: organization-defined personnel or rotes]:     Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:
IR-1	Policy and Procedures	Enterprises should integrate C-SCRM into incident response policy and procedures, and related C-SCRM Stratesy/implementation Plans and Policies. The policy and procedures must provide direction for how to address supply chain-clated incidents and cybersecurity incidents that may complicate or impact the supply chain. Individuals who work within specific mission and system environments need to recognize cybersecurity supply chain-related incidents. The incident response policy should state when and how threats and incidents should be handled, reported, and managed.	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 tikelihood or impact of future incidents.	5	fai Addresses ournose, scoe, roles, a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: [Selection (one or more): Organization-level; Mission/Dusiness process-level; System-level] incident response policy that:
IR-1	Policy and Procedures	Enterprises should integrate C-SCRM into incident response policy and procedures, and related C-SCRM States/grimplementation Plans and Policies. The policy and procedures must provide direction for how to address supply chain-related incidents and cybesecution (incidents that may complicate or impact the supply chain. Individuals who work within specific mission and system environments need to recognize cybersecutify supply chain-related incidents. The incident response policy should state when and how threats and incidents should be handled, reported, and managed.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybensecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	(a) Addresses ournose, scoe, roles, a. Develop, odcument, 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,
IR-1(1)	Policy and Procedures   C-SCRM Incident Information Sharing	Enterprises should sensure that their incident response policies and procedures provide guidance on effective information sharing or incidents and other lay risk indications in the supply chain. Culsiance should — at minimum — cover the collection, synthesis, and distribution of incident information from a divense set of data sources, such as public data mpositories, paid subscription services, and in-house threat intelligence teams. Enterprises that operate in the public sector should include specific guidance on when and how to	Functional	Intersects With	Correlation with External Organizations	IRO-02.5	Mechanisms exist to coordinate with approved third-parties to achieve a cross-organization perspective on incident awareness and more effective incident responses.	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
IR-1(1)	Policy and Procedures   C-SCRM Incident Information Sharing	communicate with interespency anteriorism, such as the ESC Endersal Accusation on two to communicate with interespency anteriorism, such as the ESC Endersal Accusation Security Council and Enterprises should ensure that their incident response policies and procedures provide guidance on effective information sharing for incidents and other key risk indicators in the supply chain. Guidance should = at a minimum – cover the collection, synthesis, and distribution of incident information from a diverse set of data sources, such as public data prepolitions, paid subscriptions enviewe, and in-hough thesi intelligence teams. Enterprises that operate in the public sector should include specific guidance on when and how to	Functional	Intersects With	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for TAAS related to the incident.	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
IR-2	Incident Response Training	Enterprises that operate in the pulsor sector should include specific guilance on views and now to communicate with interagency canters first, such as the ESC priderial Excussion Security Council and Enterprises should ensure that critical suppliers are included in incident response training. Enterprises should require their prime contraction to implement this control and flow down this requirement to relevant sub-tiler contraction. Departments and agencies should refor Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's Cybersecutity.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms suist 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;
IR-3	Incident Response Testing	Enterprises should ensure that critical suppliers are included in and/or provided with incident response testing.	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	When required by system changes; and     Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests].
IR-4	Incident Handling	Suspected cybersecurity supply chain events that may trigger an organization's C-SCRM incident handling processes. Refer to Appendix C: Task 3.4 for examples of supply chain events. C-SCRM-specific supplemental guidance is provided in control enhancements.	Functional	Equal	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (6) Endectation; and	10	a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinate incident handling activities with continency obarning activities:



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 (optional)
		This enhancement helps limit exposure of the C-SCRM information systems, networks, and processes to					Mechanisms exist to implement and govern an insider threat program.	Inntionall	
IR-4(6)	Incident Handling   Insider Threats	insider threats. Enterprises should ensure that insider threat incident handling capabilities account for the potential of insider threats associated with suppliers, envelopers, system integrators, external system service providers, and the ICI/OT-elated service providers' personnel with access to ICI/OT systems within the authorization boundary.	Functional	Intersects With	Insider Threat Response Capability	IRO-02.2		5	Implement an incident handling capability for incidents involving insider threats.
IR-4(7)	Incident Handling   Insider Threats — Intra- organization Coordination	This enhancement helps limit the exposure of C-SCRM information systems, networks, and processes to insider threats. Enterprises should ensure that insider threat coordination includes suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Intersects With	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5	Coordinate an incident handling capability for insider threats that includes the following organizational entities (Assignment: organization- defined entities).
IR-4(10)	Incident Handling   Supply Chain Coordination	A number of enterprises may be involved in managing incidents and responses for supply chain security. After initially processing the incident and deciding on a course of action (in some cases, the action may be "no action.") the enterprise may need to coordinate with thire suppliers, developen, system integrates, external system service providers, other ICT/OT-related service providers, and any relevant interagency bodies to facilitate communications, incident response, toot cause, and corrective actions. Enterprises should securely share information through a coordinated set of presents in key roles to allow for a more	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.
IR-4(10)	Incident Handling   Supply Chain Coordination	comorehensive incident handling aporoach. Selecting suppliers, developers, system integrators, external.  A number of enterprises may be involved in managing incidents and responses for supply chain security. After initiality processing the incident and deciding on a course of action (in some cases, the action may be "no action"), the enterprise may need to condinate with thirs suppliers, developers, system integrators, external system service providers, other ICTGT-related service providers, and any relevant interagency bodies to flexible communications, incident response, not cause, and corrective actions. Enterprises should securely share information through a coordinated set of personnel in key roles to allow for a more comprehensive incident handling apposes. A feeting suppliers, developers, system integrators, external.	Functional	Intersects With	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology Assess, Applications and/or services (TAXS) and other cognizations involved in the supply chain for TAAS related to the incident.	5	Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.
IR-4(11)	Incident Handling   Integrated Incident Response Team	An enterprise should include a forensics team and/or capability as part of an integrated incident response team for supply chain incidents. Where nelevant and practical, integrated incident response teams should also include necessary geographical representations aver its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Equal	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity. If and business function prepresentative that are capable of addressing cybersecurity and data protection incident response operations.	10	Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in [Assignment: organization-defined time period].
IR-5	Incident Monitoring	Enterprises should ensure that agreements with suppliers include requirements to track and document incidents, response decisions, and activities.	Functional	Equal	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	10	Track and document incidents.
IR-6	Incident Reporting	C-SCRM-specific supplemental guidance provided in control enhancement IR-6 (3).	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b. Report incident information to [Assignment: organization-defined authorities].
IR-6	Incident Reporting	C-SCRM-specific supplemental guidance provided in control enhancement IR-6 (3).	Functional	Intersects With	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	5	Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and     B. Report incident information to [Assignment: organization-defined authorities].
IR-6	Incident Reporting	C-SCRM-specific supplemental guidance provided in control enhancement IR-6 (3).	Functional	Intersects With	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	5	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b. Report incident information to [Assignment: organization-defined authorities].
IR-6(3)	Incident Reporting   Supply Chain Coordination	Communications of security incident information from the enterprise to suppliers, developers, system theigrators, external system service providers, and other ICTIOT-related service providers and vice versa require protection. The enterprise should ensure that information is reviewed and approved for sending based on its agreements with suppliers and any relevant interagency bodies. Any secalation of or exception from this reporting should be clearly defined in the agreement. The enterprise should ensure that incident reporting data is adequately protected for transmission and received by approved individuals only. Enterprise should ensure that incident reporting data is adequately protected for transmission and received by approved individuals only. Enterprises should ensure contractors to implement this control and fix does only this requirement to relevant sub-lier	Functional	Intersects With	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide or the Technology Assets, Applications not be provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for TAAS related to the incident.	5	Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.
IR-7	Incident Response Assistance	C-SCRM-specific supplemental guidance provided in control enhancement IR-7 (2).	Functional	Equal	Incident Reporting Assistance	IRO-11	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential crybersecurity and data protection incidents.	10	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.
IR-7(2)	Incident Response Assistance   Coordination with External Providers	The enterprise's agreements with prime contractors should specify the conditions under which a government- approved or -designated third party would be available or may be required to provide assistance with incident response, as well as the role and responsibility of that third party.	Functional	Equal	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	10	(a) Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability; and (b) identify organizational incident response team members to the external providers.
IR-8	Incident Response Plan	Enterprises should coordinate, develop, and implement an incident response plan that includes information- sharing responsibilities with critical supplies sed, in a federal context, interagency patrices and the FASC. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Equal	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (RP) to all stakeholders.	10	Develop an incident response plan that:     1. Provides the organization with a roadmap for implementing its incident response capability;     2. Describes the structure and organization of the incident response capability;     3. Provides a high-level approach for how the
IR-9	Information Spillage Response	The supply chain is vulnerable to information spillage. The enterprise should include supply chain-related information spillage response plan. This may require coordination with suppliers, developers, system integration, external system service providers, and other ICT/OT-related service providers. The detail of how this coordination is to be conducted should be included in the agreement (e.g., contract). Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-life contractors.	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive //egulated data spills.	5	incident response capability fits into the overall Respond to information spills by:  a. Assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills;  b. Identifying the specific information involved in the system contamination;
IR-9	Information Spillage Response	The supply chain is vulnerable to information spillage. The enterprise should include supply chain-related suformation spills in its information spillage response plan. This may require coordination with suppliers, developers, system integrators, external system service providers, and other ICT/IOT-related service providers. The details of how this coordination is to be conducted should be included in the agreement (e.g., contract). Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contracts.	Functional	Intersects With	Sensitive / Regulated Data Spill Responsible Personnel	IRO-12.1	Mechanisms exist to formally assign personnel or roles with responsibility for responding to sensitive /regulated data spills.	5	c. Alertina [Assignment: organization-defined Respond to information spills by: a. Assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills; b. Identifying the specific information involved in the system contamination;
MA-1	Policy and Procedures	Enterprises should ensure that C-SCRM is included in maintenance policies and procedures and any related SCRM Strategy/implementation Plan, SCRM Policies, and SCRM Plan(s) for all enterprise information systems and networks. With many maintenance contracts, information on mission-, enterprise, and system-specific objectives and requirements is shared between the enterprise and rise applient, developers, ystem integrators, external system service providers, and other CT/OTTestand service providers, allowing for vulnerabilities and opportunities for attack. In many cases, the maintenance of systems is outdoucted to a system integrator, administration of the strategy of the system is provided to the contract of the system is continued to the contract of the system is continued to the contract of the system integrator, and as such, appropriate measures must be taken. Even when maintenance is not applied in the system of the system of the system is contracted to the system is a contracted to the system is contracted to t	Functional	Subset Of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10	c. Alertina [Assignment: organization-defined a . Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:  (a) Addresses purpose, scope, roles,
MA-1	Policy and Procedures	Enterprises should ensure that C-SCPM is included in maintenance policies and procedures and any related SCPM Strategy/migmentation Plan, SCPM Policies, and SCPM Plan(s) for all relaterprise information relaterant and networks. With many maintenance contracts, information on mission, enterprise, and system-specific objectives and requirements is shared between the enterprise and its suppliers, developers, system integration, external system service providers, and other ICT/CTV instants are service providers, situating for contracting and such accordance in the structure of	Functional	Intersects With	Remote Maintenance Notifications	MNT-05.2	Mechanisms exist to require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time).	5	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:     I. Gelection (one or more): Organization-levet; Mission/business process-levet; System-level] maintenance policy that:     (a) Addresses purpose score roles.
MA-1	Policy and Procedures	Enterprises should ensure that C-SCRM is included in maintenance policies and procedures and any related SCRM States/grimplementation Plans, PoRP Moticies, and SCRM Plans(s) for all retriesprise information systems and networks. With many maintenance contracts, information on mission, enterprise, and system-specific objectives and requirements is shared between the enterprise and its supplient, evelopients, system-specific objectives and requirements in shared between the enterprise and its supplient, developients, system integrations, external systems reservice providers, and other ICTOTOTISEsted service providers, disnoying for systems integration, and as such approvider measurem untuke to taken. Serve where maintenance is not do no system integration, and as such approvider measurem untuke to taken. Serve where ministerance is not system integration.	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5	a. Develop, document, and disseminate to [Assignment organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:  [in] Addresses purpose, scope, roles.
MA-1	Policy and Procedures	Enterprises should ensure that C-SCPM is included in maintenance policies and procedures and any related SCPM Strategy/impermentation Plan, SCPM Policies, and SCPM Policies and procedures and any related and networks. With many maintenance contracts, information on mission, enterprise, and system-specific objectives and requirements is shared between the enterprise and its suppliers, developers, system integrators, external system sentice providers, and other ICT/OTelated service providers, allowing for vulnerabilities and opportunities for attack. In many cases, the maintenance of systems is outsourced to a large contract of the system of the sy	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	Bevelop, document, and disseminate to [Assignment: organization-defined personnel or roles]:     Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:
MA-1	Policy and Procedures	asstem integrator, and as such accordate measures must be taken. Even when maintenance is not Enterprises should ensure that C-SCRI is included in maintenance policies and procedures and any related SCRI Stategy/implementation Plan, SCRIP Policies, and SCRIP Panils (or all enterprise information systems and networks. With many maintenance constructs, information on mission-, enterprise, and system-specific objectives and requirements is shared between the enterprise and its suppliers, developers, system integrators, externs system service providers, and other ICT/TOTestated service providers, allowing for vulnerabilities and opportunities for attack. In many cases, the maintenance of systems is outdoucted to a system integrator, external as such accordance measures must be taken. Even when maintenance is not	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	In Addresses purpose, scope, roles, a. Develop, document, and disseminate to I. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: I. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that: (a) Addresses purpose, scope, roles.
MA-2	Controlled Maintenance	C-SCRM-specific supplemental guidance is provided in control enhancement MA-2 (2).	Functional	Equal	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the tilecycle of the system, application or service.	10	a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approve and monitor all maintenance activities, whether performed on site or remotely



ecure Controls Framework (SCF) 10 of 23

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM	STRM	SCF Control	SCF#	Secure Controls Framework (SCF)	Strength of	Notes (optional)
- FDE#	. DE Name	NIST SP 800-161 R1 Supplemental C-SCRM Guidance	Rationale	Relationship	oor Control	307	Control Description  Automated mechanisms exist to schedule, conduct and document	/ontionall	(a) Schedule, conduct, and document
MA-2(2)	Controlled Maintenance   Automated Maintenance Activities	Enterprises should ensure that all automated maintenance activities for supply chain systems and networks are controlled and managed according to the maintenance policy. Examples of submosted maintenance activities can include COTS product patch updates, call home features with failure notification feedback, etc. Managing these activities many require setablishing staging processes with appropriate supporting mechanisms to provide verting or filtering as appropriate. Staging processes may be especially important for critical systems and components.	Functional	Equal	Automated Maintenance Activities	MNT-02.1	maintenance and repairs.	10	maintenance, repair, and replacement actions for the system using [Assignment: organization- defined automated mechanisms]; and (b) Produce up-to date, accurate, and complete records of all maintenance, repair, and
MA-3	Maintenance Tools	Maintenance tools are considered part of the supply chain. They also have a supply chain of their own. C SCRM should be integrated when the enterprise acquires or upgrades a maintenance tool e.g., an update to the development environment or testing tool, including during the selection, ordering, storage, and integration of the maintenance tool. The enterprise should perform continuous review and approval of maintenance tools, including those maintenance tools in use by sternal service provides. The enterprise should also integrate C-SCRM when evaluating replacement parts for maintenance tools. This control may be deprived at the full vestigation of the storage of the supplementation of the supplem	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5	replacement actions requested, scheduled, in  a. Approve, control, and monitor the use of system maintenance tools; and b. Review previously approved system maintenance tools [Assignment: organization- defined frequency].
MA-3(1)	Maintenance Tools   Inspect Tools	The enterprise should deploy acceptance testing to verify that the maintenance tools of the ICT supply chain intrastructure are as expected. Maintenance tools should be authorized with appropriate paperwork, verified as c	Functional	Equal	Inspect Tools	MNT-04.1	Mechanisms exist to inspect maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.	10	Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.
MA-3(2)	Maintenance Tools   Inspect Media	The enterprise should verify that the media containing diagnostic and test programs that suppliers use on the enterprise's information systems operates as espected and provides only required functions. The use of media from maintenance tools should be consistent with the enterprise's policies and procedures and pre- approved. Enterprises should also ensure that the functionality does not exceed that which was agreed upon.	Functional	Equal	Inspect Media	MNT-04.2	Mechanisms exist to check media containing diagnostic and test programs for malicious code before the media are used.	10	Check media containing diagnostic and test programs for malicious code before the media are used in the system.
MA-3(3)		The unsubtorized removal of systems and network maintenance tools from the supply chain may introduce supply chain risks, cuch as unsubtroder modification, replement with countries, or makever invention while the tool is outside of the enterprise's control. Systems and network maintenance tools can include an integrated development environment (IDE), testing, or vulnerability scanning. For CSCRM, it improvant that enterprises should explicitly authorities, truck, and audit any removal of maintenance tools. Once systems and network tools are allowed access to an enterprise similar interprise should out of the system owner and tracked if removed and usued alseaders in the enterprise. If maintenance tools of the system owner and tracked if removed and used assessments in the enterprise. If maintenance tools were considered to the control of the system owner and tracked if removed and used assessments in the enterprise. If maintenance tools were considered to the control of the	Functional	Equal	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that containing organizational information.	10	Prevent the removal of maintenance equipment containing opanizational information by:  (a) Verifying that there is no organizational information contained on the equipment;  (b) Santizing or destroying the equipment;  (c) Retaining the equipment within the facility; or (d) Obtaining an exemention from Isassimment:
MA-4	Nonlocal Maintenance	Nonlocal maintenance may be provided by contractor personnel. Appropriate protections should be in place to manage associated risks. Controls applied to intensit maintenance personnel are applied to any suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers performing a similar maintenance role and enforced through contractual agreements with their external service providers.	Functional	Intersects With	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	5	<ul> <li>Approve and monitor nonlocal maintenance and diagnostic activities;</li> <li>b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;</li> <li>c. Employ strong suthentication in the</li> </ul>
MA-4	Nonlocal Maintenance	Nonlocal maintenance may be provided by contractor personnel. Appropriate protections should be in place to manage associated risks. Controls applied to internal maintenance personnel are applied to any suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers performing a similar maintenance role and enforced through contractual agreements with their external service providers.	Functional	Intersects With	Remote Maintenance Notifications	MNT-05.2	Mechanisms exist to require maintenance personnel to notify affected stake-holders when remote, non-local maintenance is planned (e.g., date/time).	5	a. Approve and monitor nonlocal maintenance and diagnostic activities; b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system; c. Emolov strong authentication in the
MA-4	Nonlocal Maintenance	Nonlocal maintenance may be provided by contractor personnel. Appropriate protections should be in place to manage associated risks. Controls applied to intend maintenance personnel are applied to any suppliers, developers, system integrations, attending system service providers, and other ICTOT-fested service providers performing a similar maintenance role and enforced through contractual agreements with their external service providers.	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5	Approve and monitor nonlocal maintenance and diagnostic activities;     Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;     Embly net of the system;     Embly net of the system;
MA-4(3)	Nonlocal Maintenance   Comparable Security and Sanitization	Should suppliers, developers, system integrators, outernal system service providers, or other LC/TOT-related service provides perform any norsical maintenance or diagnostic services on systems or system components, the enterprise should ensure that - Appropriate measures are taken to verify that the norlocal environment meets appropriate security levels for maintenance and diagnostics per agreements between the enterprise and vendor, - Appropriate levels of sanitizing are completed to remove any enterprise-specific data residing in commonents; and	Functional	Equal	Remote Maintenance Comparable Security & Sanitization	MNT-05.6	Mechanisms exist to require Technology Assets. Applications and/or Services (TAS) performing remote, non-local mairmenance and/or daignostic services implement a security capability comparable to the capability implemented on the system being serviced.	10	c. Emoloy strong authentication in the (a) Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or (b) Remove the component to be serviced from the swstem origin to nonlocal maintenance or
MA-5	Maintenance Personnel	Maintenance personnel may be employed by suppliers, developers, system integrators, external system service providers, or other CTGTO-related service providers. As such, appropriate protections should be in place to manage associated risks. The same controls applied to internal maintenance personnel should be applied to any contractor personnel who performs a similar maintenance role and enforced through contractual agreements with their external service providers.	Functional	Equal	Authorized Maintenance Personnel	MNT-06	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	10	s. Establish a process for maintenance personnel subtorization and maintain a list of authorized maintenance organizations or personnel;     b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and
MA-5(4)	Maintenance Personnel   Foreign Nationals	The vetting of foreign nationals with access to critical non-national security systems/renvices must take C- SCRM into account and be extended to all relevant contractor personnel. Enterprises should specify in agreements any restrictions or vetting requirements that pertain to foreign nationals and flow the requirements down to relevant subcontractors.	Functional	Intersects With	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who on these appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.	5	Ensure that: (a) Foreign nationals with appropriate security clearances are used to conduct maintenance and diagnostic activities on classified systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by
MA-6	Timely Maintenance	The enterprise should purchase spare parts, replacement parts, or alternative sources through original sequipment manufactures (DEN)s, unbrisched distributions, or subtributed resellers and ensure appropriate lead times. IT DENs are not available, it is preferred to acquire from authorized distributors. If an DEN or an authorized distributor is not available, then it is preferred to acquire from an authorized reseller. Enterprises should obtain verification on whether the distributor or reseller is authorized. Where possible, enterprises should use an authorized distributor/dealer approved list. If the only alternative is to purchase from a non- sundrotzed distributor or secondary market, a risk assessment should be performed, including revisiting the	Functional	Equal	Timely Maintenance	MNT-03	Mechanisms exist to obtain maintenance support and/or spare parts for Technology Assets, Applications and/or Services (TAAS) within a defined Recovery Time Objective (RTO).	10	Obtain maintenance support and/or spare parts for (Assignment: organization-defined system components) within (Assignment: organization-defined time period) of failure.
MA-7	Field Maintenance	Enterprises should use trusted facilities when additional rigor and quality control checks are needed, if at all practical or possible. Trusted facilities should be on an approved list and have additional controls in place.	Functional	Equal	Field Maintenance	MNT-08	Mechanisms exist to securely conduct field maintenance on geographically deployed assets.	10	Restrict or prohibit field maintenance on [Assignment: organization-defined systems or system components] to [Assignment: organization-defined trusted maintenance facilities].
MA-8	Maintenance Monitoring and Information Sharing	Tracking the failure rates of components provides useful information to the acquirer to help plan for contingencies, alternative accursed or spoy, and replacements. Failure rates are also useful for monotoring the quality and reliability of systems and components. This information provides useful feedback to suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers for corrective action and continuous improvement. In Level 2, agencies should track and communicate the failure rates to suppliers (DEM and/or an authorized distributor). The failure rates and the issues that can included staffuliers, including root causes, should be identified by an	Functional	Equal	Maintenance Monitoring	MNT-11	Mechanisms exist to maintain situational awareness of the quality and reliability of systems and components through tracking maintenance activities and component failure rates.	10	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
MA-8		Tracking the failure rates of components provides useful information to the acquirer to help plan for contingencies, laternate sources of supply, and replacements. Failure rates are also useful for monitoring the quality and reliability of systems and components. This information provides useful feedback to suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers for corrective action and continuous improvement. In Level 2, genices should treat and communicate the failure rates to suppliers (DEM and/or an authorized distributor). The failure rates and the issues that can indicate failures, including root causes should be identified by an enternite's it servicial servicine (e.g.,	Functional	Intersects With	Predictable Failure Analysis	SEA-07	Mechanisms exist to determine the Mean Time to Failure (MTTF) for system components in specific environments of operation.	5	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.
MP-1	Policy and Procedures	Various documents and information on a variety of physical and electronic media are disseminated throughout the supply chain. This information may contain a variety of tensitive information and intellectual property from suppliers, developers, spater integrators, external system service providers, and other ICT/IOT-related service providers and should be appropriately protected. Media protection policies and procedures should also address supply chain concerns, including media in the enterprise's supply chain and throughout the SDLC.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, 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/Dusiness process-level; System-level] media protection policy that:     (a) Addresses purpose, scope, roles,
MP-1	Policy and Procedures	Various documents and information on a variety of physical and electronic media are disseminated throughout the supply chain. This information may contain a variety of sensitive information and intellectual property from suppliers, developers, syber mitrigators, celemal system service providers, and other ICT/IOT-related service providers and should be appropriately protected. Media protection policies and procedures should also address supply chain concerns, including media in the enterprise's supply chain and throughout the SDLC.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:     1. [Selection (one or more): Organization-level; Mission/Dusiness process-level; System-level] media protection policy that:     (a) Addresses purpose score roles.
MP-1	Policy and Procedures	Various documents and information on a variety of physical and electronic media are disseminated throughout the supply chain. This information may contain a variety of sensitive information and intellectual property from suppliers, developers, sperim infegrators, elemand system service provides, and other ICT/IOT-salated service provides and should be appropriately protected. Media protection policies and procedures about date and dries supply chain concerns, including media in the enterprise's supply chain and throughout the SDLC.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:     [Selection (one or more): Organization-tevet; Mission/Dussiness process-levet; System-levet] media protection policy that:     [Ald Addresses purpose, scope, roles.]
MP-4	Media Storage	Media storage controls should include C-SCRM activities. Enterprises should specify and include in agreements (e.g., contracting language) media storage requirements (e.g., encryption) for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The enterprise should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Equal	Media Storage	DCH-06	Mechanisms exist to:  (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and  (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	10	a. Physically control and securely store (Assignment organization-defined types of digital and/or non-digital media) within (Assignment: organization-defined controlled areas); and b. Protect system media types defined in MP-4a until the media are destroyed or santitized using
MP-5	Media Transport	The enterprise should incorporate C-SCRM activities when media is transported by enterprise or non- enterprise personnel. Some of the techniques to protect media during transport and storage include cryptographic techniques and approved custodian services.	Functional	Equal	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	10	a. Protect and control (Assignment: organization-defined types of system media) during transport outside of controlled areas using (Assignment: organization-defined controls): b. Maintain accountability for system media during transport outside of controlled areas; c. Document activities associated with the
MP-6		Enterprises should specify and include in agreements is al., contracting language) media sanitization policies for their suppliers, developers, system integrators, external system service providers, and other CITOT- elbated service providers. Media is used throughout the SDC. Media traversing or residing in the supply chain may originate anywhere, including from suppliers, developers, system integrators, external system service providers, and other ICOT-related service providers. It can be new, refurbished, or research. Media sanitization is critical to ensuring that information is removed before the media is used, reused, or discarded. For media that contributes orishors or delter sensitive information is c. CMIT, the enterioris should require in the formedia that contributes orishors or delter sensitive information a. C. CMIT, the enterioris should require in the contributes of the contribute of the contribu	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	c. Document accurace associated with the a. Santitize flassingment: organization-defined system medial prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; and b. Employ sanitization mechanisms with the strength and integrity commensurate with the



ecure Controls Framework (SCF) 11 of 23

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM	STRM	SCF Control	SCF#	Secure Controls Framework (SCF)	Strength of Relationship	Notes (optional)
		NIST SP 800-161 R1 Supplemental C-SCRM Guidance Enterprises should specify and include in agreements (e.g., contracting language) media sanitization policies	Rationale	Relationship			Control Description  Mechanisms exist to sanitize system media with the strength and integrity	fontions II	a. Sanitize [Assignment: organization-defined
MP-6	Media Sanitization	for their suppliers, developers, system integrators, external system service providers, and other ICI/OT- leathed service providers. Media is used throughout the SDC, Media traversing or residing in the supply chain may originate anywhere, including from suppliers, developers, system integrators, external system service providers, and other ICI/OT-related service providers. It can be new, thruthshed, or reused. Media samilization is critical to ensuring that information is removed before the media is used, reused, or discarded.	Functional	Intersects With	System Media Sanitization	DCH-09	commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; and b. Employ sanitization mechanisms with the
MP-6	Media Sanitization	For modia that contains orivacy or other sensitive information (e.g., CUIL the enterprise should require its Enterprises should specify and include in agreements (e.g., contracting language) media santization policies for their suppliers, developers, system integratore, external system service providers, and other ICT/OT- related service providers. Media is used introughout the SDLC, Media traversing or residing in the supply chain may originate anywhere, including from suppliers, developers, system integratore, external system service providers, and other ICT/OT-related service providers. It can be now, refluitables, or reused. Media santization is critical to ensuring that information is removed before the media is used, reused, or discarded, For media that contains univacy or other sensitive information (e.g., CUIL, the enteriories should require in for media that contains univacy or other sensitive information (e.g., CUIL).	Functional	Intersects With	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	5	strenath and integrity commensurate with the a. Sanitize flasignment organization-defined system media) prior to disposal, release out of organizational control, or release for reuse using [Assignment organization-defined sanitization techniques and procedures]; and b. Employ sanitization mechanisms with the strength and integrity commensurate with the
PE-1	Policy and Procedures	The enterprise should integrate C-SCRM practices and requirements into their own physical and environmental protection policy and procedures. The degree of protection should be commensurate with the degree of integration. The physical and environmental protection policy and procedures. The degree of protection should be commensurate with the degree of integration. The physical and environmental protection policy should ensure that the physical interfaces of the supply chain have developed protection and audit to such protection.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	sucritud and meeting comments and dispersion with the S. Develop, document, and dispersional to (Assignment organization-defined personnel or roles):  1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy
PE-1	Policy and Procedures	The enterprise should integrate C-SCRM practices and requirements into their own physical and environmental protection policy and procedures. The degree of protection should be commensurate with the degree of integration. The physical and environmental protection policy should ensure that the physical interfaces of the supply chain have adequate protection and audit for such protection.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	that: a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/Dusiness process-level; System-level] physical and environmental protection policy
PE-1	Policy and Procedures	The enterprise should integrate C-SCRM practices and requirements into their own physical and environmental protection policy and procedures. The degree of protection should be commensurate with the degree of integration. The physical and environmental protection policy should ensure that the physical interfaces of the supply chain have adequate protection and audit for such protection.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or It significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	inst:  3. Develop, document, and disseminate to [Assignment: organization-defined personnel or rotes]:  1. [Selection (one or more): Organization-level; Mission/Dusiness process-level; System-level] physical and environmental protection policy that:
PE-2	Physical Access Authorizations	Enterprises should ensure that only authorized individuals with a need for physical access have access to information, systems, or data center, e.g., enseithe or closeling. Such authorizations should speely what the individual is permitted or not permitted to do with negard to their physical access (e.g., iven abert-configure, insert something, connect something, remove, etc.). Agreements should address physical access authorization requirements, and the enterprise should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Authorization for not-deteral employees should flow an approved anotoco, which includes documentation of the authorization and	Functional	Equal	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with subcrited access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	10	a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides; b. Issue authorization credentials for facility soccess; c. Review the access list detailing authorized facility access by individuals [Assistment:
PE-2(1)	Physical Access Authorizations   Access by Position or Role	Role-based authorizations for physical access should include federal (e.g., agency/department employees) and non-federal employees (e.g. suppliers, developers, system integrators, external system service providers, and orbit (CT/OT-related service providers). When role-based authorization is used, the type and level of access allowed for that role or position must be pre-established and documented.	Functional	Equal	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	10	Authorize physical access to the facility where the system resides based on position or role.
PE-3	Physical Access Control	Physical access control should include individuals and enterprise engaged in the enterprise's supply chain. A vetting process based on enterprise-defined requirements and policy should be in place pitor to granting access to the supply chain infrastructure and any relevant elements. Access establishment, maintenance, and revocation processes should meet enterprise access control policy riger. The speed of revocation for suppliers, developers, system integrations, external systems envice providers, and other ICT/IOT-related service providers who need access to physical facilities and data centers – either enterprise owned or external spering envider owned and access to physical facilities and data centers.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entrylext) points) for Societies (excluding those areas within the facility officially designated as publicly accessible).	5	Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by:     Verifying individual access authorizations before granting access to the facility; and C. Controllini increase and exerces to the facility.
PE-3(1)	Physical Access Control   System Access	physical access controls should be extended to contractor personnel. Any contractor resources that provid services support with physical access to the supply chain infrastructure and any relevant elements should adhere to access controls. Policies and procedures should be consistent with those applied to employee personnel with similar levels of physical access.	Functional	Equal	Access To Information Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility.	10	Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [Assignment organization-defined physical spaces containing one or more components of the system].
PE-3(2)	Physical Access Control   Facility and Systems	When determining the extent, frequency, and/or randomness of security checks of facilities, enterprises should account for exfiltration risks that result from covert listening devices. Such devices may include wiretaps, roving bugs, cell sits simulators, and other eavesdropping technologies that can transfer sensitive information out of the enterprise.	Functional	Intersects With	Physical Access Control	PES-03	Physicial access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	Perform security checks [Assignment: organization-defined frequency] at the physical perimeter of the facility or system for extiltration of information or removal of system components.
PE-3(5)	Physical Access Control   Logical Tampering   Protection	Tamper protection is critical for reducing cybenecurity risk in products. The enterprise should implement validated tamper protection techniques within the supply chair. For critical products, the enterprise should sequile and assess whether and to what dearest a supplier has implemented tamper protection mechanisms. Resource and the sequile control of the cont	Functional	Equal	Mobile Device Tampering	MDM-04	Mechanisms exist to protect mobile devices from tampering through inspecting devices returning from locations that the organization deems to be of significant risk, prior to the device being connected to the organization's network.	10	Employ [Assignment: organization-defined anti- tamper technologies] to [Selection (one or more): detect; prevent] physical tampering or alteration of [Assignment: organization-defined hardware components] within the system.
PE-6	Monitoring Physical Access	solividuals who physically access the enterprise or external service provider's facilities, data centers, information, or physical assets) - including via the supply-tain—may be employed by the enterprise's employees, on-site or remotely located contractors, viators, other third parties (e.g., maintenance personnel under contract with the contractor enterprise, or an individual diffiliated with an enterprise in the upstream supply chain. The enterprise should monitor these individuals' activities to reduce cybersecurity risks throughout the supply chain or require monothing in agreement.	Functional	Equal	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	10	a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents; b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events! and
PE-16	Delivery and Removal	This control enhancement reduces cybersecurity risks that arise during the physical delivery and removal of hardware components from the enterprise's information systems or supply chain. This includes transportations seem, when we have the component of the component of samilization present the component of the component of the component of the component of queristical, or maintenance environment (e.g., classified integration and test taboratory).	Functional	Equal	Delivery & Removal	PES-10	Physical security mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access.	10	a. Authorize and control [Assignment: organization-defined types of system components] entering and exiting the facility; and b. Maintain records of the system components.
PE-17	Alternate Work Site	The enterprise should incorporate protections to guard against cybersecurity risks associated with enterprise employees or contractor personnel within or accessing the supply chain infrastructure using atternative work sites. This can include third-party personnel who may also work from alternative worksites.	Functional	Equal	Alternate Work Site	PES-11	Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	10	a. Determine and document the [Assignment: organization-defined alternate work sites] sillowed for use by employees;     b. Employ the following controls at alternate work sites: [Assignment: organization-defined controls]:     c. Assess the effectiveness of controls at
PE-18	Location of System Components	Physical and environmental hazards or disruptions have an impact on the availability of products that are or will be acquired and physically transported to the enterprise's locations. For example, enterprises should incorporate the manufacturing, warehousing, or the distribution location of information system components that are critical for agency operations when planning for alternative suppliers for these components.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	Position system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.
PE-20	Asset Monitoring and Tracking	The enterprise should, whenever possible and practical, use asset location technologies to track systems and components transported between entitles corcus the supply calin, between protected areas, or in storage awaiting implementation, testing, maintenance, or disposal. Methods include RFID, digital signatures, or blockchains. These technologies help protect against.  a. Diverting the system or component for counterfeit replacement; b. The loss of confidentiality, integrity, or availability of the system or component function and data (including).	Functional	Equal	Asset Monitoring and Tracking	PES-14	Physical security mechanisms exist to employ asset location technologies that track and monitor the location and movement of organization-defined assets within organization-defined controlled areas.	10	Employ [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas].
PE-23	Facility Location	Enterprises should incorporate the facility location (e.g., data centern) when assessing risks associated with suppliers. Factors may include geographic location (e.g., of princinated lurised States (CONUS), Diviside the Continental Lurised states (CONUS), Division and a control of such facilities, environments having potential (e.g., located in a high-risk selsimic zone), and alternative facility locations. Enterprises should also assess whether the location of annual facility locations. Enterprises should such assesses whether the location of annual facility locations. Enterprises should such assesses whether the location of a manufacturing of distribution center could be influenced by geographical, economic, or other factors. For	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5	Plan the location or site of the facility where the system resides considering physical and environmental hazards; and     b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.
PE-23	Facility Location	Enterprises should incorporate the facility location (e.g., data certen) when assessing risks associated with suppliers. Factors may include geographic coloration (e.g., commental United States (CONUS), Dutside the Continental United States (CONUS), Dutylocal protections in place at one or more of the relevant facilities. Cool ammangement and control of such reliabilities, environmental hazard potential (e.g., located in a highlies, sesimic zone), and alternative facility locations. Enterprises should also assess whether the location of ammantacturing or distribution center could be influenced by appositional, excorning, or other factors. For	Functional	Intersects With	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	5	Plan the location or site of the facility where the system resides considering physical and environmental hazards; and b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.
PE-23	Facility Location	critical vendros or products, enterentiese should a socialised for address any requirements or restrictions Enterprises should incorporate the facility location (e.g., do the centrel) when assessing irisks associated with suppliers. Factors may include geographic location (e.g., Continental United States (CONUS), Dutatide the Continental United States (CONUS), physical productions in place at one or more of the relevant facilities, local management and control of such facilities, environmental hazard potential (e.g., located in a high-risk sessinic zone), and attenuithe facilities (actions. Enterprises should also assess whether the location of manufacturing or distribution center could be influenced by geogoditical, economic, or other factors. For critical vendros or goodscts, enterprises should associated widers any requirements or restrictions.	Functional	Intersects With	Alternate Storage Site	BCD-08	Mechanisms exist to establish an alternate storage site that includes both the assets and recessary agreements to permit the storage and recovery of system backup information.	5	Plan the location or site of the facility where the system resides considering physical and environmental hazards; and b. For existing facilities, consider the physical and environmental hazards in the organizational
PE-23	Facility Location	Enterior terroptice or produces, memorines around sessional autoress alor producers and reterroptices. Terreprises should incorporate the facility location (e.g., desired enterin) when sessesing risks associated with suppliers. Factors may include geographic location (e.g., Continental United States (CONUS), Outside the Continental United States (CONUS), privical productions in place at one or more of the relevant facilities, local transgement and control of such facilities, environmental hazard potential (e.g., located in a high-risk seismic zone), and attenuable facilities (autorities and control of such facilities, environmental hazard potential (e.g., located in a high-risk seismic zone), and attenuable facilities (autorities and control of such facilities, environmental hazard potential (e.g., located in a high-risk seismic zone), and attenuable facilities (autorities and control of such activities of the seismic zone), and whether the location of manufacturing or distribution centre could be influenced by geopolitical, economic, or other factors. For critical vendors or conducts, enterorises should searchically address any reculterments or restrictions	Functional	Intersects With	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.	5	Plan the location or site of the facility where the system resides considering physical and environmental hazards; and b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.
PE-23	Facility Location	Send in trades to ut could, the international across sense in tradestinated and the sense in the	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	Plan the location or site of the facility where the system resides considering physical and environmental hazards; and     b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.



ecure Controls Framework (SCF) 12 of 23

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM	STRM	SCF Control	SCF#	Secure Controls Framework (SCF)	Strength of Relationship	Notes (optional)
		NIST SP 800-161 R1 Supplemental C-SCRM Guidance Enterprises should incorporate the facility location (e.g., data centers) when assessing risks associated with	Rationale	Relationship			Control Description  Mechanisms exist to facilitate the operation of physical and environmental	/ontionall	a. Plan the location or site of the facility where
PE-23	Facility Location	suppliers. Factors may include geographic location (e.g., Continental United States (CONUS), Outside the Continental United States (CONUS), pylical protections in place at one or more of the relevant facilities, local management and control of such facilities, environmental hazard potential (e.g., located in a high-risk seismic zone), and attensitie facility colosions. Enterprises about also assess whether the location of amanufacturing or distribution center could be influenced by geopolitical, economic, or other factors. For ordical vanders or goodsets, enterprises should searching address any requirements or restrictions	Functional	Intersects With	Physical & Environmental Protections	PES-01	protection controls.	5	<ol> <li>rean the location or site or the facility where the system resides considering physical and environmental hazards; and</li> <li>For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.</li> </ol>
PL-1	Policy and Procedures	The security planning policy and procedures should integrate C-SCRY. This includes creating, disseminating, and updating the security policy, operational policy, and procedures for C-SCRY to his practical expectations of the control of the contro	Functional	Subset Of	Cybersecurity & Data Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection-related resource planning controls that define a viable plan for achieving cybersecurity and data protection objectives.	10	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:     1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:
PL-1	Policy and Procedures	The security planning policy and procedures should integrate C-SCRM. This includes creating, disseminating, and updating the security policy, operational policy, and procedures for C-SCRM to shape acquisition or development requirements and the follow on implementation, operations, and maintenance of systems, system interfaces, and network connections. The C-SCRM policy and procedures provide inputs tinto and task paid interfaces, and network connections. The C-SCRM policy and procedures provide inputs tinto and task paid interfaces, and network connections. The C-SCRM policy and procedures provide inputs tinto an account of the connection of the conne	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	(a) Addresses purpose, scope, roles, a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selication (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:
PL-1	Policy and Procedures	SCRM plan at Level 3, in Level 4, ensure that the full SDLC is covered from the C-SCRM perspective.  The security planning policy and procedures should integrate C-SCRM. This includes creating, disseminating, and updating the security policy, operations policy, and procedures for C-SCRM to shape acquisition or development requirements and the follow-on implementation, operations, and maintenance of systems, system interfaces, and network connections. The C-SCRM Story and procedures provide inputs this or and take guidance from the C-SCRM Strategy and implementation Plan at Level 1 and the System Security Plan and C-SCRM plan at Level 3. In Level 3, ensure that the full SDLC is covered from the C-SCRM perspective.	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Nechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	(a) Addresses purpose, scope, rofes,  Develop, document, and tilsseminate to [Assignment: organization-defined personnel or roles]:  1. [Selication (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:
PL-1	Policy and Procedures	The security planning policy and procedures should integrate C-SCRM. This includes creating, disseminating, and updating the security policy, operational policy, and procedures for C-SCRM to shape acquisition or development requirements and the follow-on implementation, operations, and maintenance of systems, system interfaces, and network connections. The C-SCRM policy and procedures provide inputs into and take guidance from the C-SCRM Strategy and Implementation Plan at Level 1 and the System Security Plan and C-SCRM plant at Level 3. In Level 3, ensure that the full SDCL is covered from the C-SCRM perspective.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals of It significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	(a) Addresses purpose, scope, roles, a Develop, document, and disseminate to (Assignment: organization-defined personnel or roles):  [. Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:  [. Addresses purpose, scope, roles,]
PL-1	Policy and Procedures	The security planning policy and procedures should integrate C-SCRM. This includes creating, disseminating, and updating the security policy, operational policy, and procedures for C-SCRM to shape acquisition or development requirements and the follow-on implementation, operations, and maintenance of systems, system interfaces, and retwork connections. The C-SCRM policy and procedures provide inputs this or and take guidance from the C-SCRM Strategy and implementation Plan at Level 1 and the System Security Plan and C-SCRM policy Level. 3. In Level 3, ensure that the full SDCL is covered from the C-SCRM perspective.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	Isl Addresses purpose, scope, rotes, a. Develop, document, and disseminate to (Assignment organization-defined personnel or rotes):  1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:  (a) Addresses purpose, scope, rotes.
PL-2	System Security and Privacy Plans	The system security plan (SSP) should integrate C-SCRM. The enterprise may choose to develop a stand- olation C-SCRM plan for an individual system or integrate SCRM controls into their SSP. The system security plan and/or system-level C-SCRM plan provide inputs into and take guidance from the C-SCRM Strategy and implementation Plan at Level 1 and the C-SCRM policy at Level 1 and Level 2. In addition to internal coordination, the emergines should coordinate with suppliers, developers, system integrators, external system service providers, and other ICT/IOT-related service providers to develop and maintain their SSPs. For searnole, building and ocerating a switter requires a similarity occurrent coordination and collaboration between the	Functional	Intersects With	Plan / Coordinate with Other Organizational Entities	IAO-03.1	Mechanisms exist to plan and coordinate Information Assurance Program (IAP) activities with affected stakeholders before conducting such activities in order to reduce the potential impact on operations.	5	a. Develop security and privacy plans for the system that:  1. Are consistent with the organization's enterprise architecture;  2. Explicitly define the constituent system components;  3. Describe the operational context of the system
PL-2	System Security and Privacy Plans	The system security plans (SSP) should integrate C-SCRM. The enterprise may choose to develop a stand- one C-SCRM plan for an individual system or integrate SCRM controls into their SSP. The system security plan and/or system-level C-SCRP plan provide inputs into and take guidance from the C-SCRM Strategy and implementation Flant at level 1 and the C-SCRM policy at the control of the control o	Functional	Intersects With	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical Technology Assets, Applications and/or Services (TAAS), as well as influence inputs, entities and TAAS, providing a historical record of the data and its origins.	5	Describe the oberational context of the system a. Develop security and privacy plans for the system that:     1. Are consistent with the organization's enterprise architecture;     2. Explicitly define the constituent system components;     3. Describe the operational context of the system.
PL-2	System Security and Privacy Plans	examels. building and operating a system requires a sinfficant coordination and collaboration between the The system security plant RSP9 should integrate C-SCRM. The enterprise may chose to develop a stand- alone C-SCRM plant for an individual system or integrate SCRM controls into their SSP. The system security plant and/or system level C-SCRM plant provide inproxis into and take guidance from the C-SCRM strategy and implementation Plant at Level 1 and the C-SCRM policy at Level 1 and Level 2. In addition to internal coordination, the enterprise should coordinate with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to develop and maintain their SSPs. For seamles, building and operating a system requires a similfraint coordination and collaboration between the system service providers, and other ICT/OT-related service providers to develop and maintain their SSPs. For seamles, building and operating a system requires a similfraint coordination and collaboration between the system service providers.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient destalt to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5	a. Develop security and privacy plans for the system that:  1. Are consistent with the organization's enterprise architecture;  2. Explicitly define the constituent system components;  3. Describe the operational context of the system
PL-4	Rules of Behavior	The rules of behavior apply to contractor personnel and internal agency personnel. Contractor enterprises are responsible for ensuring that their employees follow applicable rules of behavior. Individual contractors should not be granted access to agency systems or data until they have acknowledged and demonstrated compliance with this control. Failure to meet this control can result in the removal of access for such individuals.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work.	5	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy; b. Receive a documented acknowledgment from such individuals, indicating that they have read,
PL-4	Rules of Behavior	The rules of behavior apply to contractor personnel and internal agency personnel. Contractor enterprises are responsible for ensuring that their employees follow applicable rules of behavior. Inclindual contractors should not be garded access to agency systems or data until they have acknowledge and demonstrated compliance with this control. Failure to meet this control can result in the removal of access for such inclinduals.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy; b. Receive a documented acknowledgment from such individuals, indicating that they have read.
PL-4	Rules of Behavior	The rules of behavior apply to contractor personnel and internal agency personnel. Contractor enterprises are responsible for ensuring that their employees follow applicable rules of behavior. Inclindual contractors should not be garded access to agency systems or data until they have acknowledge and demonstrated compliance with this control. Failure to meet this control can result in the removal of access for such inclinduals.	Functional	Intersects With	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy; b. Receive a documented acknowledgment from such individuals, indicating that they have read.
PL-7	Concept of Operations	The concept of operations (CONOPS) should describe how the enterprise intends to operate the system from the perspective of C-SCRH. It should integrate C-SCRH and be managed and updated throughout the applicable system's SDLC to address cybersecurity risks throughout the supply chain.	Functional	Equal	Security Concept Of Operations (CONOPS)	OPS-02	Nechanisms exist to develop a security Concept of Operations (CONOPS), or a similarly-defined plan for achieving cybersecurity objectives, that documents management, operational and technical measures implemented to apply defense-in-depth techniques that is communicated to all appropriate stakeholders.	10	a. Develop a Concept of Operations (CONOPS) for the system describing how the organization intends to operate the system from the perspective of information security and privacy; and b. Review and update the CONOPS [Assignment: organization-defined frequency].
PL-8	Security and Privacy Architectures	Security and privacy architecture defines and directs the implementation of security and privacy-protection methods, mechanisms, and capabilities to the underlying systems and networks, as well as the information system that is being created. Security and exhibitions in a consider interpretation of the security is built-in throughout the SDLC. Enterprises should consider implementing zero-trust architectures and should ensure that security is exhibited units of the source of the security and should ensure that security architecture is well understood by system developent-fregineers and system security engineers. This control applies to both federal agency and non-federal agency employees. Supplier deversity privates options for addressing information security and supply chain concerns. The	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Nechanisms exist to develop an enterprise architecture, sligned with industry-recognized leading practices, with consideration for cybersecurity and data protection principles that addresses risk to organizational operations, assets, inclviduals, other organizations.	5	a. Develop security and privacy architectures for the system that:  1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;  2. Describe the requirements and approach to be taken for processing personally identifiable
PL-8(2)	Security and Privacy Architectures   Supplier Diversity	support overantly provides options or soldreshing information security and supply creat concerns. Are enterprises should incorporate this control as it relates to supplies, developes, pulse infigerations, seternal system service provides, and other ErrOT-related service provides.  The enterprises should plan for the potential replacement of suppliers, developers, system integrators, external system service providers, and other ICTOT-related service provides in case one is no longer abel to meet the enterprise should be a resultinger to a command one of the plantses of other one meet contractual.	Functional	Intersects With	Supplier Diversity	TDA-03.1	Mechanisms exist to obtain cybersecurity and data protection technologies from different suppliers to minimize supply chain risk.	5	Require that [Assignment: organization-defined controls] allocated to [Assignment: organization-defined locations and architectural (syers) are obtained from different suppliers.
PL-9	Central Management	C-SCRM controls are managed centrally at Level 1 through the CSCRM Strategy and Implementation Plan and at Level 1 and Level 2 through the C-SCRM Ploticy. The C-SCRM PMO described in Section 2 centrally manages C-SCRM controls at Level 1 and Level. At Level 3, C-SCRM controls are managed on an information system basis through the SSP and/or CSCRM Plan.	Functional	Intersects With	Centralized Management of Cybersecurity & Data Protection Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of cybersecurity and data protection controls and related processes.	5	Centrally manage (Assignment: organization- defined controls and related processes).
PL-9	Central Management	C-SCRM controls are managed centrally at Level 1 through the CSCRM Strategy and implementation Plan and at Level 1 and Level 2 through the C-SCRM Policy. The C-SCRM PMO described in Section 2 centrally manages C-SCRM controls at Level 1 and Level. At Level 3, C-SCRM controls are managed on an information system basis though the SSP and/or CSCRM Plan.	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	Centrally manage [Assignment: organization- defined controls and related processes].
PL-9	Central Management	CSCRM controls are managed centrally at Level 1 through the CSCRM Strategy and implementation Plan and at Level 1 and Level 2 through the CSCRM Policy. The CSCRM PMO described in Section 2 centrally manages CSCRM controls at Level 1 and Level. At Level 3, C-SCRM controls are managed on an information system basis though the SSP and/or CSCRM Plan.	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program.	5	Centrally manage [Assignment: organization- defined controls and related processes].
PL-9	Central Management	C-SCRM controls are managed centrally at Level 1 through the CSCRM Strategy and implementation Plan and at Level 1 and Level 2 through the C-SCRM Policy. The C-SCRM PMO described in Section 2 centrally manages C-SCRM controls at Level 1 and Level. At Level 3, C-SCRM controls are managed on an information system basis though the SSP and/or CSCRM Plan.	Functional	Intersects With	Centralized Management of Antimalware Technologies	END-04.3	Mechanisms exist to centrally-manage antimalware technologies.	5	Centrally manage [Assignment: organization-defined controls and related processes].
PL-9	Central Management	C-SCRM controls are managed centrally at Level 1 through the CSCRM Strategy and implementation Plan and at Level 2 through the C-SCRM Policy. The C-SCRM PMO described in Section 2 centrally manages C-SCRM controls at Level 1 and Level. At Level 3, C-SCRM controls are managed on an information system basis though the SSP and/or CSCRM Plan.	Functional	Intersects With	Central Management	END-08.1	Mechanisms exist to centrally-manage anti-phishing and spam protection technologies.	5	Centrally manage [Assignment: organization-defined controls and related processes].
PL-9	Central Management	C-SCRM controls are managed centrally at Level 1 through the CSCRM Strategy and Implementation Plan and at Level 2 through the C-SCRM Portion, The C-SCRM PMO described in Section 2 centrally manages C-SCRM controls at Level 1 and Level. At Level 3, C-SCRM controls are managed on an information system basis though the SSP and/or CSCRM Plan.	Functional	Intersects With	Centralized Management of Planned Audit Record Content	MON-03.6	Nechanisms exist to centrally manage and configure the content required to be captured in audit records generated by organization-defined system components.	5	Centrally manage (Assignment: organization- defined controls and related processes).



Secure Controls Framework (SCF) 13 of 23

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 (optional)
		·					Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS)	(ontional)	
PL-10	Baseline Selection	Enterprises should include C-SCRM controls in their control baselines. Enterprises should identify and select C-SCRM controls based on the C-SCRM requirements identified within each of the Wesh. A. C-SCRM brown was assist in identifying C-SCRM control baselines that meet common C-SCRM requirements for different groups, communities of interest, or the enterprise as a whole	Functional	Equal	Secure Baseline Configurations	CFG-02	that are consistent with industry-accepted system hardening standards.	10	Select a control baseline for the system.
PM-2	Information Security Program Leadership Role	The senior information security officer (e.g., CISD) and senior agency official responsible for acquisition (e.g., Clief Acquisition (Inteller, CRQI) or senior Pocuments Executive (SFE) have key exponsibilities for CRPM and the overall cross-enterprise coordination and collaboration with other applicable senior personnel within the enterprise, such as the CIO, the head of facilities physical security, and the risk security function). This coordination should occur regardless of the specific department and agency enterprise structure and specific titles of network service and specific structure. The coordination could be secured by the C-SCRMPMO or another similar function. Section 2 provides more suitatione on C-SCRM Prior and responsibilities.	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and recorrects to centrally manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program.	5	Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.
PM-3	Information Security and Privacy Resources	An enterprise's C-SCRM program requires dedicated, sustained funding and human resources to successfully implement agency C-SCRM requirements. Section 3 of this document provides guidance on dedicated hunding for C-SCRM programs. The enterprise should also integrate CSCRM requirements into major IT investments to ensure that funding aporporating significant through the capital planning and provided to the control of the section and improve the investory or legislate, a management efficiency of the enterprise's supply chain, section and improve the investory or legislate, an anagement efficiency of the enterprise's supply chain, section and improve the investory or legislate, an anagement efficiency of the enterprise's supply chain,	Functional	Equal	Cybersecurity & Data Protection Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity and data protection programs and document all exceptions to this requirement.	10	a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement; b. Prepare documentation required for addressing information security and privacy roorarms in coalital clanning and investment
PM-4	Plan of Action and Milestones Process	C-SCIM items should be included in the POABM at all levels. Digardations should develop POABMs based on C-SCIM seasoned reports. POABM should be used by organizations to describe planned actions to correct the deficiencies in C-SCIM controls identified during assessment and the continuous monitoring of progress against those actions.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:      Are developed and maintained;     Document the remedial information security.
PM-4	Plan of Action and Milestones Process	C-SCRM items should be included in the POA&M st all levels. Organizations should develop POA&Ms based on C-SCRM assessment reports. POA&M should be used by organizations to describe planned actions to correct the deficiencies in C-SCRM controls identified during assessment and the continuous monitoring of progress against those actions.	Functional	Intersects With	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses of deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:      1. Are developed and maintained;      2. Document the remedial information security.
PM-5	System Inventory	Having a current system inventory is foundational for C-SCRN. Not having a system inventory may lead to the enterprise's inability to identify system and supplier criticality, which would result in an inability to conduct C-SCRN activities. To canneur that all applicable suppliers are identified and categorized for criticality, enterprises should relievent supplier information in the system inventory and maintain its currency and accuracy. Enterprises should regive their primer contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Departments and agencies should regive having the contractors of the primer contractors to implement the insolation in accordance with Executive Order 14028, Improvint in Nation's Obsersecutiv,	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	Develop and update [Assignment: organization- defined frequency] an inventory of organizational systems.
PM-5	System Inventory	Induction I use a spatient in another behalf because the Control of the Control o	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and for 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:	5	Develop and update [Assignment: organization- defined frequency] an inventory of organizational systems.
PM-6	Measures of Performance	Enterprises should use measures of performance to track the implementation, efficiency, effectiveness, and expect of CSCBM activities. The CSCBM PMO is responsible for creating CSCBM measures of performance is collaboration with other applicable stackholders to include iterativity fine spengrogate audience and decision makers and providing guidance on data collection, analysis, and reporting.	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program.	5	Develop, monitor, and report on the results of information security and privacy measures of performance.
PM-6	Measures of Performance	Enterprises should use measures of performance to track the implementation, efficiency, effectiveness, and impact of C-SCRM activities. The C-SCRM PMO is responsible for creating C-SCRM measures of performance in collaboration with other applicable stakeholders to include identifying the appropriate audience and decision makers and providing guidence on data collection, analysis, and reporting.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	5	Develop, monitor, and report on the results of information security and privacy measures of performance.
PM-7	Enterprise Architecture	C-SCRM should be integrated when designing and maintaining enterprise architecture.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity and data protection principles that addresser init to organizational operations, assets, individuals, other organizations.	5	Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.
PM-8	Critical Infrastructure Plan	C-SCRM should be integrated when developing and maintaining critical infrastructure plan	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (CODP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.
PM-8	Critical Infrastructure Plan	C-SCRM should be integrated when developing and maintaining critical infrastructure plan	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.
PM-9	Risk Management Strategy	The risk management strategy should address cybersecurity risks throughout the supply chain. Section 2, Appendix C, and Appendix D of this document provide guidance on integrating C-SCRN into the risk management strategy.	Functional	Equal	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	Develops a comprehensive strategy to manage:      Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and     Privacy risk to individuals resulting from the
PM-10	Authorization Process	C-SCRM should be integrated when designing and implementing authorization processes.	Functional	Equal	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection assessment and authorization controls.	10	a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes; b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk meanagement process: and
PM-11	Mission and Business Process Definition	The enterprier's mission and business processes should address cybenecurity risks throughout the supply chair. When addressing mission and business process definitions, the enterprise should ensure that C-SCPM activities are incorporated into the support processes for achieving mission success. For example, a system supporting a critical mission function that has been designed and implemented for easy removal and replacement should a component fail in syequite the use of somewhat unresibled herviews components. A C- SCPM activity may need to be defined to ensure that the supplier makes component spare parts readily available for excellent the supplier makes component spare parts readily available for excellent this need to the supplier makes component spare parts readily available for excellent this need to the supplier makes component spare parts readily available for excellent this need to the supplier makes component spare parts readily available for excellent this need to the supplier makes component spare parts readily available for excellent this need to the supplier makes component spare parts readily available for excellent this need to the supplier makes component spare parts readily available for excellent this need to the supplier makes component spare parts readily available for excellent this need to the supplier makes component to the supplier makes compone	Functional	Equal	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of notate-trion needs is orbitalized.	10	Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and     Determine information protection and
PM-12	Insider Threat Program	An insider threat program should include C-SCRM and be tailored for both federal and non-federal agency individuals who have access to agency systems and networks. This control applies to contractors and subcontractors and should be implemented throughout the SDLC.	Functional	Equal	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross-discipline insider threat incident handling team.	10	Implement an insider threat program that includes a cross-discipline insider threat inclident handling team.
PM-13	Security and Privacy Workforce	Security and privacy workforce development and improvement should ensure that relevant C-SCRM topics are integrated into the content and initiatives produced by the program. Section 2 provides information on C- SCRM roles and responsibilities. NISTSP 800-161 can be used as a source of topics and activities to include in the security and privacy workforce program.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	Establish a security and privacy workforce development and improvement program.
PM-13	Security and Privacy Workforce	Security and privacy workforce development and improvement should ensure that relevant C-SCRM topics are integrated into the content and initiatives produced by the program. Section 2 provides information on C- SCRM roles and responsibilities. NIST SP 800-161 can be used as a source of topics and activities to include in the security and privacy workforce program.	Functional	Intersects With	Cybersecurity & Data Protection-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	Establish a security and privacy workforce development and improvement program.
PM-14	Testing, Training, and Monitoring	The enterprise should implement a process to ensure that organizational plans for conducting supply chain risk testing, training, and monitoring activities associated with organizational systems are maintained. The C-SCRP PMO can provide guidance and support on how to integrate C-SCRM into testing, training, and monitoring plans.	Functional	Intersects With	Testing, Training & Monitoring	PRI-08	Mechanisms exist to conduct cybersecurity and data protection testing, training and monitoring activities	5	a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems. I have developed and maintained; and 2. Continue to be executed; and a Designation training training and an administration training and monitoring plans.
PM-14	Testing, Training, and Monitoring	The enterprise should implement a process to ensure that organizational plans for conducting supply chain risk testing, training, and monitoring activities associated with organizational systems are maintained. The C-SCR	Functional	Intersects With	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.	5	b. Review testins, trainins, and monitoring olans a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:  1. Are developed and maintained; and 2. Continue to be executed; and b. Review testins, training, and monitoring clans
PM-15	Security and Privacy Groups and Associations	Contact with security and privacy groups and associations should include C-SCRM practitioners and those with C-SCRM responsibilities. Acquisition, tegal, critical infrastructure, and supply chain groups and associations should be incorporated. The C-SCRM PMO can help identify agency personnel who could benefit from participation, specific groups to participate in, and relevant topics.	Functional	Intersects With	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-barrier capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	Establish and institutionalize contact with selected groups and associations within the security and privacy communities: a. To facilitate ongoing security and privacy education and training for organizational personnel; b. To maintain currency with recommended



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)	Strength of Relationship	Notes (optional)
		Contact with security and privacy groups and associations should include C-SCRM practitioners and those	Nationate	neadonamp			Mechanisms exist to establish contact with selected groups and associations within the cybersecurity and data protection communities to:	(ontional)	Establish and institutionalize contact with selected groups and associations within the
PM-15	Security and Privacy Groups and Associations	with C-SCRM resolutions and supply chain groups and associations should be incorporated. The C-SCRM PMO can help identify agency personnel who could benefit from participation, specific groups to participate in, and relevant topics.	Functional	Intersects With	Contacts With Groups & Associations	GOV-07	(1) Facilitate ongoing cybersecurity and data protection education and training for organizational personnet; (2) Maintain currency with recommended cybersecurity and data protection practices, techniques and technologies; and Calabara C	5	security and privacy communities: a. To facilitate ongoing security and privacy education and training for organizational personnel; b. To maintain currency with recommended
PM-16	Threat Awareness Program	A threat awareness program should include threats that emanate from the supply chain. When addressing supply chain threat awareness, knowledge should be shared between stakeholden within the boundaries of the enterprise's information sharing policy. The C-SCRM PMO can help identify C-SCRM stakeholders to include in threat information sharing, a swell as potential sources of information for supply chain threats.	Functional	Intersects With	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.
PM-17	Protecting Controlled Unclassified Information on External Systems	The policy and procedures for controlled unclassified information (CUI) on external systems should include protecting relevant supply chain information. Conversely, it should include protecting agency information that resides in external systems because such external systems are part of the agency supply chain.	Functional	Equal	Protecting Sensitive Data on External Systems	DCH-13.3	Mechanisms exist to ensure that the requirements for the protection of sensitive information processed, stored or transmitted on external Technology Assets, Applications and/or Services (TAKS), are implemented in accordance with applicable statutory, regulatory and contractual obligations.	10	a. Establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies,
PM-18	Privacy Program Plan	The privacy program plan should include C-SCRM. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant subtler contractors.	Functional	Equal	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	recutations, and standards: and a. Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency's privacy program, and:  1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program are overview of the requirements for 2. Provides an overview of the requirements for
PM-19	Privacy Program Leadership Role	The privacy program leadership role should be included as a stakeholder in applicable C-SCRM initiatives and activities.	Functional	Equal	Chief Privacy Officer (CPO)	PRI-01.1	Mechanisms exist to appoint a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and excurses to coordisate, develop and implement, applicable led also privacy requirements and manage data privacy risks through the organization-wide data privacy program.	10	Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.
PM-20	Dissemination of Privacy Program Information	The dissemination of privacy program information should be protected from cybersecurity risks throughout the supply chain.	Functional	Equal	Dissemination of Data Privacy Program Information	PRI-01.3	Mechanisms exist to:  (i) Ensure that the public has access to information about organizations of data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar rote;  (g) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories;  (ii) Itilizia multiful facilization and websites or document repositories;  (iii) Itilizia multiful facilization and websites and/or other lines to anable.	10	Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that: a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior.
PM-21	Accounting of Disclosures	An accounting of disclosures should be protected from cybersecurity risks throughout the supply chain.	Functional	Equal	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PO) controlled by:  (1) The organization; and/or  (2) Relevant third-parties that their PD was shared with.	10	Develop and maintain an accurate accounting of disclosures of personally identifiable information, including:     1. Date, nature, and purpose of each disclosure; and     2. Name and address, or other contact referential or this patient is a segmentation to.
PM-22	Personally Identifiable Information Quality Management	Personally identifiable information (PII) quality management should take into account and manage cybersecurity risks related to PII throughout the supply chain.	Functional	Intersects With	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	5	Information of the individual or organization to Develop and document organization-wide policies and procedures for: a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle;
PM-22	Personally Identifiable Information Quality Management	Personally identifiable information (PII) quality management should take into account and manage cybersecurity risks related to PII throughout the supply chain.	Functional	Intersects With	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, limeliness, impact, completeness and de-identification of information throughout the information lifecycle.	5	b. Correctins or deletine inaccurate or outdated Develop and document organization-wide policies and procedures for: a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle;
PM-23	Data Governance Body	Data governance body is a stakeholder in C-SCRM and should be included in cross-agency collaboration and information sharing of C-SCRM activities and initiatives (e.g., by participating in inter-agency bodies, such as the FASC).	Functional	Intersects With	Data Management Board	PRI-13	Mechanisms exist to establish a written charter for a Data Management Board (DMB) and assigned organization-defined roles to the DMB.	5	Correcting or deleting inaccurate or outdated     Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].
PM-23	Data Governance Body	Data governance body is a stakeholder in C-SCRM and should be included in cross-agency collaboration and information sharing of C-SCRM activities and initiatives (e.g., by participating in inter-agency bodies, such as the FASC).	Functional	Intersects With	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	5	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].
PM-23	Data Governance Body	Data governance body is a stakeholder in C-SCRM and should be included in cross-agency collaboration and information sharing of C-SCRM activities and initiatives (e.g., by participating in inter-agency bodies, such as the FASC).	Functional	Intersects With	Data Governance	GOV-10	Mechanisms exist to facilitate data governance to oversee the organization's policies, standards and procedures so that sensitive/regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.	5	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	Supply chain-related cybersecurity risks to personally identifiable information should be addressed by the minimization policies and procedures described in this control.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purposely originally collected, consistent with the data privacy noticely): (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual politications.	5	a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research; b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes:
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	Supply chain-related cybersecurity risks to personally identifiable information should be addressed by the minimization policies and procedures described in this control.	Functional	Intersects With	Collection Minimization	END-13.3	Mechanisms exist to utilize sensors that are configured to minimize the collection of information about individuals.	5	a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research; b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research ourcoses:
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	Supply chain-related cybersecurity risks to personally identifiable information should be addressed by the minimization policies and procedures described in this control.	Functional	Intersects With	Minimize Visitor Personal Data (PD)	PES-06.5	Mechanisms exist to minimize the collection of Personal Data (PD) contained in visitor access records.	5	a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research; b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research ournoses:
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	Supply chain-related cybersecurity risks to personally identifiable information should be addressed by the minimization policies and procedures described in this control.	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.	5	a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research; b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	Supply chain-related cybersecurity risks to personally identifiable information should be addressed by the minimization policies and procedures described in this control.	Functional	Intersects With	Limit Sensitive / Regulated Data In Testing, Training & Research	DCH-18.2	Mechanisms exist to minimize the use of sensitive/regulated data for research, testing, or training, in accordance with authorized, legitimate business practices.	5	a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research; b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes:
PM-26	Complaint Management	Complaint management process and mechanisms should be protected from cybersecurity risks throughout the supply chain. Enterprises should also integrate C-SCRM security and privacy controls when fielding complaints from vendors or the general public (e.g., departments and agencies fielding inquiries related to exclusions and removals).	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization confects, receives, processes, stores, transmits, shares, updates and/or disposes of their Personal Data (PD).	5	Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes: a. Mechanisms that are easy to use and readily
PM-26	Complaint Management	Compilaint management process and mechanisms should be protected from cybersecurity risks throughout the supply chain. Enterprises should also integrate C-SCRM security and privacy controls when fielding compilaints from vendors or the general public (e.g., departments and agencies fielding inquiries related to exclusions and removals).	Functional	Intersects With	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	5	accessible by the public: Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes: a. Mechanisms that are easy to use and readily
PM-27	Privacy Reporting	Privacy reporting process and mechanisms should be protected from cybersecurity risks throughout the supply chain.	Functional	Equal	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that cover collecting, receiving, processing, storing, transmitting, updating, sharing and disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	10	accessible by the oublic:  a. Develop [Assignment: organization-defined privacy reports] and disseminate to:  1. [Assignment: organization-defined oversight bodies] to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and  2. [Assignment: organization-defined officials]
PM-28	Risk Framing	C-SCRM should be included in risk framing. Section 2 and Appendix C provide detailed guidance on integrating C-SCRM into risk framing.	Functional	Equal	Risk Framing	RSK-01.1	Nechanisms exist to identify:  (1) Assumptions affecting risk assessments, risk response and risk monitoring;  (2) Constraints affecting risk assessments, risk response and risk monitoring;  (3) The organizational risk tolerance; and  (4) The organizational risk tolerance; and	10	Nesterment contactor related on the contactor of the



ture Controls Framework (SCF) 15 of 23

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 (optional)
PM-29	Risk Management Program Leadership Roles	Risk management program leadership roles should include C-SCRM responsibilities and be included in C- SCRM collaboration across the enterprise. Section 2 and Appendix C provide detailed guidance for C-SCRM roles and responsibilities	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TARS), including documenting selected mitigating actions and monitoring performance against those plans.	(ontional)	a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes: and b. Establish a Risk Executive (function) to view
PM-29	Risk Management Program Leadership Roles	Risk management program leadership roles should include C-SCRM responsibilities and be included in C- SCRM collaboration across the enterprise, Section 2 and Appendix C provide detailed guidance for C-SCRM roles and responsibilities	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to entrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program.	5	and anakvz risk from an organization-wide a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and b. Establish a Risk Executive (function) to view
PM-29	Risk Management Program Leadership Roles	Risk management program leadership rotes should include C-SCRM responsibilities and be included in C- SCRM collaboration across the enterprise. Section 2 and Appendix C provide detailed guidance for C-SCRM roles and responsibilities	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	and analyze risk from an oranization-wide a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and b. Establish a Risk Executive (function) to view
PM-30	Supply Chain Risk Management Strategy	The Supply Chain Risk Management Strategy (also known as C-SCRM Strategy) should be complemented with a C-SCRM Implementation Plan that tay out detailed initiatives and activities for the enterprise with timelines and responsible parties. This implementation plan can be a POAMA for be included in a POAMA stage with C-SCRM Strategy and Implementation Plan at Level 1, the enterprise should select and document common C- SCRM controls that should address the enterprise, program, and system-specific reseds. These controls should be iteratively integrated into the C-SCRM Policy at Level 1 and Level 2, as well as the C-SCRM plan (or	Functional	Equal	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TARS), including documenting selected mitigating actions and monitoring performance against those plans.	10	and anakvz risk from an orsanization-wide a. Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services; 1. Implement the supply chain risk management
PM-31	Continuous Monitoring Strategy	SSP If required) at Level 3. See Section 2 and Appendix C for further guidance on risk management.  The continuous monitoring strategy and program should integrate CSCRM controls at Levels 1, 2, and 3 in accordance with the Supply Chain Risk Management Strategy.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	strategy consistently across the organization; Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include: a. Establishing the following organization-wide metrics to be monitored: [Assignment: organization-defined metrics]; b. Establishing fassignment: organization-
PM-32	Purposing	Extending systems assigned to support specific mission or business functions beyond their initial purpose subjects those systems to unintentional risks, including cybersecurity risks throughout the supply chain. The application of this control should include the explicit incorporation of cybersecurity supply chain exposures.	Functional	Equal	Purpose Validation	GOV-11	Mechanisms exist to monitor mission/business-critical Technology Assets, Applications and/or Services (TAAS) to ensure those resources are being used consistent with their intended purpose.	10	Analyze [Assignment: organization-defined systems or systems components] supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.
PS-1	Policy and Procedures	As each lawel, the personnel security policy and procedures and the related C SCRM Strategylimplementation Pan, C SCRM Policies, and C SCRM Plan(s) need to define the roles for the personnel who are engaged in the acquisition, management, and execution of supply chain security activities. These roles also need to state acquirer personnel responsibilities with regard to relationships with suppliers, developers, system integrators, external system service providers, and other CT/T-chelded service providers. Publicies and procedures need to consider the full system development life cycle of systems and the roles and responsibilities respect to address the various supplice which infrastructure schildring.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	Develop, document, and disseminate to [Assignment: organization-defined personnel or rotes]:     [Selection (one or more): Organization-level;     Mission/Dusiness process-level; System-level]     personnel security policy that:     [Addissers purpose score rotes
PS-1	Policy and Procedures	At each level, the personnel security policy and procedures and the related C-SCRM Strategy/implementation Pan. C-SCRM Policies, and C-SCRM Parily need to define the roles for the personnel who are engaged in the acquisition, management, and execution of supply chain security activities. These roles also need to state acquirer personnel responsibilities with regard for relationships with suppliers, developers, system integrators, external system service providers, and other ICT/IOT-related service providers. Policies and concodures need to consider the full service development (leve cold or statems and the roles and to conduct sented to consider the full service development (leve cold or statems and the roles and	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	fal Addresses Durnose, scone, roles. a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/Dusiness process-level; System-level] personnel security policy that:
PS-1	Policy and Procedures	issonabilities needed to address the various supply chain infrastructure schivities.  At each level, the personnel security policy and procedures and the related C-SCRM Strategy/implementation Pan, C-SCRM Policies, and C-SCRM Plani(s) need to define the roles for the personnel who are engaged in the acquisition, management, and execution of supply chains exceptive activities. These roles also need to strate acquirer personnel responsibilities with regard to relationships with suppliers, developers, system integrators, external system an existence and entire CTOT-related service providers. Publicies and procedures need to consider the full system development life cycle of systems and the roles and responsibilities needed to address the various supply which infrastructure schivities.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	(a) Addresses ournose, scoes, roles.  a. Develop, document, and disseminate to (Assignment: organization-defined personnel or roles):  [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that:  (a) Addresses purpose, scooe, roles.
PS-3	Personnel Screening	To mitigate insider threat risk, personnel screening policies and procedures should be extended to any contractor personnel with authorized access to information systems, system components, or information system services. Continuous monitoring activities should be commensurate with the contractor's level of access to sensitive, classified, or regulated information and should be consistent with broader enterprise policies. Screening requirements should be incorporated into agreements and flow down to sub-tier contractors	Functional	Equal	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	Screen individuals prior to authorizing access to the system; and     D. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening].
PS-6	Access Agreements	The enterprise should define and document access agreements for all contractors or other external personnel win namy need to access the enterprise's data, systems, or relevok, whether physically or logically. Access agreements should state the appropriate level and method of access to the information system and supply chain network. Additionally, terms of access should be considered with the enterprise's information security policy and may need to specify additional restrictions, such as allowing access during specific timeframes, them specific locations, or only by personnel who have statisfied additional vetting requirements. The	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	5	a. Develop and document access agreements for organizational systems; b. Review and update the access agreements (Assignment: organization-defined frequency); and c. Verify that individuals requiring access to accessive information and or access.
PS-6	Access Agreements	externises bould declore south mechanisms to review, monitor, uodate, and track access by these parties in the enterprise should define and document access agreements for all contractors or other external present with many need to access the enterprise's data, systems, or network, whether physically or logically. Access agreements should state the appropriate level and method of access to the information system and support chain network. Additionally, terms of access should be consistent with the enterprise's information security policy and may need to specify additional restrictions, such as allowing access during specific timethames, from specific locations, or orby by personne who have astalfied additional vetting requirements. The	Functional	Intersects With	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	5	organizational information and systems: a. Develop and document access agreements for organizational systems; b. Review and update the access agreements [Jassignment: organization-defined frequency]; and c. Verify that individuals requiring access to
PS-7	External Personnel Security	seterories should declore audit mechanisms to review, monitor, undete, and track access to these admiss in Mick garby personnel who have access to be enterprise is immediately approximation systems and entrooks must make the same personnel security requirements as enterprise personnel. Examples of such third-party personnel can include the system integrants, developers, pupplier, external service provider used for develoy, contractors or service providers who are using the ECTOT systems, or supplier maintenance personnel brought in to address component technical issues not solvable by the enterprise or system integrator.	Functional	Equal	Third-Party Personnel Security	HRS-10	Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party cybersecurity and data protection roles and responsibilities.	10	organizational information and systems: a. Establish personnel security requirements, including security roles and responsibilities for external providers; b. Require external providers to comply with personnel security policies and procedures established by the organization:
PT-1	Policy and Procedures	Enterprises should ensure that supply chain concerns are included in PII processing and transparency policies and procedures, as well as the nelated C-SCRM Strategy/Implementation Plan, C-SCRM Policies, and C-SCRM Plan. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies.  The procedures can be established for the security and privacy program in general and individual information	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	Document personnel security requirements:     Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:     [Selection (one or more): Organization-level; Mission/business process-level; System-level] personally identifiable information processing
PT-1	Policy and Procedures	systems. These colic van derocedures should address the surrose, accose, rides, responsibilities. Enterprises should ensure that supply hair occerns are included in Pil processing and transparency policies and procedures, as well as the related C-SCRM Strategy/Implementation Plan, C-SCRM Policies, and C-SCRM Plan. The policy can be included as processed and the processed of the policies.  The procedures can be established for the security and privacy policy are to the procedures can be established for the security and privacy program in general and individual information	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	and transparency policy that:  a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:  1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personally identifiable information processing
PT-1	Policy and Procedures	avatems. These solic vand corcedures should addiests the aurose, acoos, roles, responsibilities. Etterprises should ensure that supply behan concerns are included in PB processing and transparency policies and procedures, as well as the related C-SCRM Strategy/Implementation Plan, C-SCRM Policies, and C-SCRM Plan. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies.  The procedures can be established for the security and privacy program in general and individual information systems. These policy and procedures should address the prope, acoop, criose, seponsibilities,	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recopitzed cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	and transasency colicy that:  a. Develop, document, and disseminate to [Assignment organization-defined personnel or roles]: [I. Selection (one or more): Organization-level; Mission/business process-level; System-level] personally identifiable information processing and transparency policy that:
RA-1	Policy and Procedures	Risk assessments should be performed at the enterprise, mission/program, and operational levels. The system-level risk assessment should include both the supply chain infrastructure (e.g., development and testing environments and delivery systems) and the information system/components traversing the supply call. System-level risk assessments significantly intersect with the SDIC and should complement the enterprise is broader 6PF architics, which take part during the SDIC or Actuality analysis will ensure that common/self. The system of	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals of sligitizant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	Develop, document, and disseminate to [Assignment organization-defined personnel or roles]:     [Selection (one or more): Organization-tevel; Mission/business process-level; System-level] risk assessment policy that:     (a) Addresses purpose, scoee, roles.
RA-1	Policy and Procedures	Risk assessments should be performed at the enterprise, mission/program, and operational levels. The system-level risk assessment should include both the supply chain infrastructure (e.g., development and leasting environments and delivery systems) and the information systemicomponents traversing the supply chain. System-level risk assessments significantly intersect with the SDC and should complement the enterprise's broader RPM activities, which take part during the SDC. A criticality analysis will ensure that mission-critical functions and components are given higher priority due to their impact on the mission, if commonised. The Goolie should include subole chainelevant contensessor to research as a socialisation of commonised. The state are social social relationships.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	Develop, document, and disseminate to [Assignment organization-defined personnel or roles]:     [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that:     [Ald Addresses purpose, scope, roles,
RA-1	Policy and Procedures	Risk assessments should be performed at the enterprise, mission/program, and operational levels. The system-level risk assessment should include both the supply-chain infrastructure (e.g., development and testing environments and delivery systems) and the information system/components traversing the supply chain. System-level risk assessments significantly intersect with the SDLC and should complement the enterprise's broader RFF activities, who take part during the SDLC. A criticality analysis will ensure that mission-critical functions and components are given higher priority due to their impact on the mission, if compromised. The Gools' should include supply chains content of the size	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:     [Selection (one or more): Organization-tevel; Mission/business process-level; System-level] risk assessment policy that:     (a) Addresses purpose, scooe, roles.
RA-2	Security Categorization	Security categorization is critical to C-SCRM at Levels 1, 2, and 3. In addition to [FIPS 199] categorization, security categorization for C-SCRM should be based on the criticality analysis that is performed as part of the SDLC. See Section 2 and [NISTR 8179] for a detailed description of criticality analysis.	Functional	Equal	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, registations and contractual obligations that:  (1) Document the security categorization results (including supporting rationals) in the security categorization results (including supporting rationals) in the security plant for yet) services; and (2) Ensure the security categorization decision is reviewed and approved by the nester cares.	10	a. Categorize the system and information it processes, stores, and transmitts;     b. Document the security categorization results, including supporting rationale, in the security plan for the system; and c. Verify that the authorizing official desinated reorsesntative reviews and
RA-3	Risk Assessment	Risk assessments should include an analysis of drifticality, threats, vulnerabilities, likelihood, and impact, as described in dealin in Appendix. C. The data to be reviewed and collected includes CSRP4-specific ross, processes, and the results of system/component and senices acquisitions, implementation, and integration. Risk assessments should be performed at levels 1, 2 and 3. Risk assessments in higher levels should consist primarily of a synthesis of various risk assessments performed at lower levels and used for undestanding the overall impact with the level (a.g., at the enterprise or mission/function levels). C-SRM risk assessments should concilement and inform ski assessments, which are dendrimed as oracinar of the described of the control of th	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for attheence to the organization's cybersecurity and data protection policies and standards.	5	a. Conduct a risk assessment, including: <ol> <li>I. Identifying threats to and vulnerabilities in the system;</li> <li>Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system. the information it processes, stores, or</li> </ol>



cure Controls Framework (SCF) 16 of 23

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM	STRM	SCF Control	SCF#	Secure Controls Framework (SCF)	Strength of Relationship	Notes (optional)
		NIST SP 800-161 R1 Supplemental C-SCRM Guidance Risk assessments should include an analysis of criticality, threats, vulnerabilities, likelihood, and impact, as described in detail in Appendix C. The data to be reviewed and collected includes C-SCRM-specific roles.	Rationale	Relationship			Control Description  Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use,	Inntionall	a. Conduct a risk assessment, including:     1. Identifying threats to and vulnerabilities in the
RA-3	Risk Assessment	described in detail in Appendix C. The data to be reviewed and collected includes C-SCRM-specific roles, processes, and the results of system/component and services acquisitions, implementation, and integration. Risk assessments should be performed at Levels 1, 2, and 3. Risk assessments at higher levels should	Functional	Intersects With	Risk Assessment	RSK-04	the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	Identifying threats to and vulnerabilities in the system;     Determining the likelihood and magnitude of
		consist primarily of a synthesis of various risk assessments performed at lower levels and used for understanding the overall impact with the level (e.g., at the enterprise or mission/function levels). C-SCRM					rectinology resetts, representations, sectioned and or settle (170-60).		harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the
		risk assessments should complement and inform risk assessments, which are performed as ongoing Vulnerability monitoring should cover suppliers, developers, system integrators, external system service					Mechanisms exist to detect vulnerabilities and configuration errors by		system, the information it processes, stores, or a. Monitor and scan for vulnerabilities in the
RA-5	Vulnerability Monitoring	providers, and other ICT/OT-related service providers in the enterprise's supply chain. This includes employing data collection tools to maintain a continuous state of awareness about potential vulnerability to	Functional	Intersects With	Vulnerability Scanning	VPM-06	routine vulnerability scanning of systems and applications.	5	system and hosted applications [Assignment: organization-defined frequency and/or randomly
RA-S	and Scanning	suppliers, as well as the information systems, system components, and raw inputs that they provide through the cybersecurity supply chain. Vulnerability monitoring activities should take place at all three levels of the enterprise. Scoping vulnerability monitoring activities requires enterprises to consider suppliers as well as	Functional	intersects with	vulnerability Scanning	VPM-U6		5	in accordance with organization-defined process] and when new vulnerabilities
		enterprise. Scoping vulnerability monitoring activities requires enterprises to consider suppliers as well as their sub-suppliers. Enterprises, where applicable and appropriate, may consider providing customers with a Vulnerability monitoring should cover suppliers, developers, system integrators, external system service					Mechanisms exist to update vulnerability scanning tools.		potentially affecting the system are identified and reported: a. Monitor and scan for vulnerabilities in the
	Vulnerability Monitoring	providers, and other ICT/OT-related service providers in the enterprise's supply chain. This includes employing data collection tools to maintain a continuous state of awareness about potential vulnerability to							system and hosted applications [Assignment: organization-defined frequency and/or randomly
RA-5	and Scanning	suppliers, as well as the information systems, system components, and raw inputs that they provide through the cybersecurity supply chain. Vulnerability monitoring activities should take place at all three levels of the	Functional	Intersects With	Update Tool Capability	VPM-06.1		5	in accordance with organization-defined process] and when new vulnerabilities
		enterprise. Scoping vulnerability monitoring activities requires enterprises to consider suppliers as well as their sub-suppliers. Enterprises, where applicable and appropriate, may consider providing customers with a					Mechanisms exist to identify the breadth and depth of coverage for		potentially affecting the system are identified and reported:
	Vulnerability Monitoring	Enterprises that monitor the supply chain for vulnerabilities should express the breadth of monitoring based on the criticality and/or risk profile of the supplier or product/component and the depth of monitoring based					Mechanisms exist to identify the breadth and depth of coverage for vulnerability scanning that define the system components scanned and types of vulnerabilities that are checked for.		
RA-5(3)	and Scanning   Breadth and Depth of Coverage	on the level of the supply chain at which the monitoring takes place (e.g., sub-supplier). Where possible, a component inventory (e.g., hardware, software) may aid enterprises in capturing the breadth and depth of the	Functional	Equal	Breadth / Depth of Coverage	VPM-06.2	types of vulnerabilities that are checked for.	10	Define the breadth and depth of vulnerability scanning coverage.
		products/components within their supply chain that may need to be monitored and scanned for vulnerabilities							
	Vulnerability Monitoring						Automated mechanisms exist to compare the results of vulnerability scans over time to determine trends in system vulnerabilities.		
RA-5(6)	and Scanning   Automated Trend	Enterprises should track trends in vulnerabilities to components within the supply chain over time. This information may help enterprises develop procurement strategies that reduce risk exposure density within the supply chain.	Functional	Equal	Trend Analysis	VPM-06.4		10	Compare the results of multiple vulnerability scans using [Assignment: organization-defined automated mechanisms].
	Analyses	the supply chain.							automated mechanisms j.
		Enterprises should integrate capabilities to respond to cybersecurity risks throughout the supply chain into					Mechanisms exist to respond to findings from cybersecurity and data protection assessments, incidents and audits to ensure proper		
RA-7	Risk Response	the enterprise's overall response posture, ensuring that these responses are aligned to and fall within the boundaries of the enterprise's tolerance for risk. Risk response should include consideration of risk response	Functional	Equal	Risk Response	RSK-06.1	remediation has been performed.	10	Respond to findings from security and privacy assessments, monitoring, and audits in
		identification, evaluation of alternatives, and risk response decision activities							accordance with organizational risk tolerance.
		Enterprises should complete a criticality analysis as a prerequisite input to assessments of cybersecurity supply chain risk management activities. First, enterprises should complete a criticality analysis as part of					Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a		Identify critical system components and
RA-9	Criticality Analysis	the Frame step of the C-SCRM Risk Management Process. Then, findings generated in the Assess step activities (e.g., criticality analysis, threat analysis, vulnerability analysis, and mitigation strategies) update	Functional	Intersects With	Third-Party Criticality	TPM-02	supply chain risk assessment process relative to their importance in supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	functions by performing a criticality analysis for [Assignment: organization-defined systems,
		and tailor the criticality analysis. A symbiotic relationship exists between the criticality analysis and other Assess step activities in that they inform and enhance one another. For a highquality criticality analysis,			Assessments		supporting the delivery of ingrivation delivers.	-	system components, or system services] at [Assignment: organization-defined decision
		enterprises should employ it iteratively throughout the SLDC and concurrently across the three levels.  Enterprises should complete a criticality analysis as a prerequisite input to assessments of cybersecurity					Mechanisms exist to require the developer of the system, system		points in the system development life cycle].  Identify critical system components and
		supply chain risk management activities. First, enterprises should complete a criticality analysis as part of the Frame step of the C-SCRM Risk Management Process. Then, findings generated in the Assess step	_				component or service to perform a criticality analysis at organization- defined decision points in the Secure Development Life Cycle (SDLC).		functions by performing a criticality analysis for [Assignment: organization-defined systems,
RA-9	Criticality Analysis	activities (e.g., criticality analysis, threat analysis, vulnerability analysis, and mitigation strategies) update and tailor the criticality analysis. A symbiotic relationship exists between the criticality analysis and other	Functional	Intersects With	Criticality Analysis	TDA-06.1		5	system components, or system services] at [Assignment: organization-defined decision
		Assess step activities in that they inform and enhance one another. For a highquality criticality analysis, enterorises should emotor it iteratively throughout the SLDC and concurrently across the three levels. Enterprises should complete a criticality analysis as a prerequisit input to assessments of cybersecurity					Mechanisms exist to identify critical system components and functions by		points in the system development life cycle].
		supply chain risk management activities. First, enterprises should complete a criticality analysis as part of the Frame step of the C-SCRM Risk Management Process. Then, findings generated in the Assess step			Cybersecurity & Data		performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the		Identify critical system components and functions by performing a criticality analysis for
RA-9	Criticality Analysis	activities (e.g., criticality analysis, threat analysis, vulnerability analysis, and mitigation strategies) update and tailor the criticality analysis. A symbiotic relationship exists between the criticality analysis and other	Functional	Intersects With	Protection Requirements Definition	PRM-05	Secure Development Life Cycle (SDLC).	5	[Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision
		Assess step activities in that they inform and enhance one another. For a highquality criticality analysis, enterorises should emotor it iteratively throughout the SLDC and concurrently across the three levels.							points in the system development life cycle].
		The C-SCRM threat hunting activities should supplement the enterprise's internal threat hunting activities. As a critical part of the cybersecurity supply chain risk management process, enterprises should actively monitor for threats to their supply chain. This requires a collaborative effort between C-SCRM and other cyber					Mechanisms exist to perform cyber threat hunting that uses indicators of Compromise (loC) to detect, track and disrupt threats that evade existing security controls.		a. Establish and maintain a cyber threat hunting capability to:     1. Search for indicators of compromise in
RA-10	Threat Hunting	defense-oriented functions within the enterprise. Threat hunting capabilities may also be provided via a shared services enterprise, especially when an enterprise lacks the resources to perform threat hunting	Functional	Equal	Threat Hunting	THR-07	security controls.	10	organizational systems; and 2. Detect, track, and disrupt threats that evade
		activities themselves. Typical activities include information sharing with peer enterprises and actively consuming threat intelligence sources (e.g., like those available from Information Assurance and Analysis							existing controls; and b. Employ the threat hunting capability
		The system and services acquisition policy and procedures should address C-SCRM throughout the acquisition management life cycle process, to include purchases made via charge cards. C-SCRM					Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to		Develop, document, and disseminate to     [Assignment: organization-defined personnel or
SA-1	Policy and Procedures	procurement actions and the resultant contracts should include requirements language or clauses that address which controls are mandatory or desirable and may include implementation specifications, state	Functional	Subset Of	Technology Development & Acquisition	TDA-01	meet unique business needs.	10	roles]: 1. [Selection (one or more): Organization-level;
		what is accepted as evidence that the requirement is satisfied, and how conformance to requirements will be verified and validated. C-SCRM should also be included as an evaluation factor.							Mission/business process-level; System-level] system and services acquisition policy that: (a) Addresses purpose, scope, roles.
		The system and services acquisition policy and procedures should address C-SCRM throughout the acquisition management life cycle process, to include purchases made via charge cards. C-SCRM					Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned		a. Develop, document, and disseminate to [Assignment: organization-defined personnel or
SA-1	Policy and Procedures	procurement actions and the resultant contracts should include requirements language or clauses that address which controls are mandatory or desirable and may include implementation specifications, state	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection	GOV-03	intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	roles]: 1. [Selection (one or more): Organization-level;
		what is accepted as evidence that the requirement is satisfied, and how conformance to requirements will be verified and validated. C-SCRM should also be included as an evaluation factor.			Program				Mission/business process-level; System-level] system and services acquisition policy that:
		The system and services acquisition policy and procedures should address C-SCRM throughout the acquisition management life cycle process, to include purchases made via charge cards. C-SCRM					Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).		(a) Addresses purpose, scope, roles, a. Develop, document, and disseminate to [Assignment: organization-defined personnel or
SA-1	Policy and Procedures	procurement actions and the resultant contracts should include requirements language or clauses that address which controls are mandatory or desirable and may include implementation specifications, state	Functional	Intersects With	Secure Software Development Practices	TDA-06	Development Plactices (SSDP).	5	roles]: 1. [Selection (one or more): Organization-level;
		what is accepted as evidence that the requirement is satisfied, and how conformance to requirements will be verified and validated. C-SCRM should also be included as an evaluation factor.			(SSDP)				Mission/business process-level; System-level] system and services acquisition policy that:
							Mechanisms exist to identify and allocate resources for management,		(a) Addresses purpose, scope, roles, a. Determine the high-level information security
		The enterprise should incorporate C-SCRM requirements when determining and establishing the allocation of					operational, technical and data privacy requirements within business process planning for projects / initiatives.		and privacy requirements for the system or system service in mission and business process
SA-2	Allocation of Resources	resources.	Functional	Equal	Allocation of Resources	PRM-03		10	planning; b. Determine, document, and allocate the resources required to protect the system or
		There is a strong relationship between the SDLC and C-SCRM activities. The enterprise should ensure that C-					Mechanisms exist to manage the usable lifecycles of technology assets.		system service as part of the organizational a. Acquire, develop, and manage the system
	System Development	SCRM activities are integrated into the SDLC for both the enterprise and for applicable suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. In addition			Technology Lifecycle				using [Assignment: organization-defined system development life cycle] that incorporates
SA-3	Life Cycle	to traditional SDLC activities, such as requirements and design, the SDLC includes activities such as inventory management, acquisition and procurement, and the logical delivery of systems and components.	Functional	Intersects With	Management	SEA-07.1		5	information security and privacy considerations; b. Define and document information security and
		See Section 2 and Appendix C for further guidance on SDLC. Departments and agencies should refer to Accendix F to implement this guidance in accordance with Executive Order 14028. Improving the Nation's There is a strong relationship between the SDLC and C-SCRM activities. The enterprise should ensure that C-					Manhaniama aviat ta angura ahangan ta Taghaniam, Assata Angliagtiana		privacy roles and responsibilities throughout the system development life cycle: a. Acquire, develop, and manage the system
	0	There is a strong relationship between the SDLC and C-SCHM activities. The enterprise should ensure that C- SCRM activities are integrated into the SDLC for both the enterprise and for applicable suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. In addition			Secure Development Life		Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.		using [Assignment: organization-defined system development life cycle] that incorporates
SA-3	System Development Life Cycle	to traditional SDLC activities, such as requirements and design, the SDLC includes activities such as inventory management, acquisition and procurement, and the logical delivery of systems and components.	Functional	Intersects With	Cycle (SDLC) Management	PRM-07		5	information security and privacy considerations; b. Define and document information security and
		See Section 2 and Appendix C for further guidance on SDLC. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028, Improving the Nation's							privacy roles and responsibilities throughout the system development life cycle;
		Enterprises are to include C-SCRM requirements, descriptions, and criteria in applicable contractual agreements.			Minimum Viable Product		Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product		Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract
SA-4	Acquisition Process	Enterprises are to establish baseline and tailorable C-SCRM requirements to apply and incorporate into contractual agreements when procuring a product or service from suppliers, developers, system integrators,	Functional	Intersects With	(MVP) Security Requirements	TDA-02	technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	[Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for
		external system service providers, and other ICT/OT-related service providers.  These include but are not limited to:	<u></u>						the system, system component, or system service:
		Enterprises are to include C-SCRM requirements, descriptions, and criteria in applicable contractual agreements.	-				Mechanisms exist to facilitate the implementation of third-party management controls.		Include the following requirements, descriptions, and criteria, explicitly or by reference, using
SA-4	Acquisition Process	Enterprises are to establish baseline and tailorable C-SCRM requirements to apply and incorporate into	Functional	Intersects With	Third-Party Management	TPM-01		5	[Selection (one or more): standardized contract language; [Assignment: organization-defined
		contractual agreements when procuring a product or service from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.							contract language]] in the acquisition contract for the system, system component, or system
		These include but are not limited to: Enterprises are to include C-SCRM requirements, descriptions, and criteria in applicable contractual agreements.					Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to		service: Include the following requirements, descriptions, and criteria, explicitly or by reference, using
SA-4	Acquisition Process	Enterprises are to establish baseline and tailorable C-SCRM requirements to apply and incorporate into	Functional	Intersects With	Technology Development & Acquisition	TDA-01	meet unique business needs.	5	[Selection (one or more): standardized contract language; [Assignment: organization-defined
		contractual agreements when procuring a product or service from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.			a Acquisition				contract language]] in the acquisition contract for the system, system component, or system
		These include but are not limited to: Enterprises are to include C-SCRM requirements, descriptions, and criteria in applicable contractual					Mechanisms exist to control changes to services by suppliers, taking into		service: Include the following requirements, descriptions,
SA-4	Acquisition Process	agreements.  1. Enterprises are to establish haseline and tailorable C-SCRM requirements to annly and incorporate into	Functional	Intersects With	Managing Changes To	TPM-10	account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	5	and criteria, explicitly or by reference, using [Selection (one or more): standardized contract
3A-4	Acquisición Process	<ol> <li>Enterprises are to establish baseline and tailorable C-SCRM requirements to apply and incorporate into contractual agreements when procuring a product or service from suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.</li> </ol>	runctional	microects with	Third-Party Services	1FM-10			language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system
		external system service providers, and other ICT/OT-related service providers.  These include but are not limited to:					Mechanisms exist to ensure vendors / manufacturers:		service: Require the developer of the system, system
	Acquisition Process I	If an enterprise needs to purchase components, they need to ensure that the product specifications are "fit			Pre-Established Secure		(1) Deliver the system, component, or service with a pre-established, secure configuration implemented; and		component, or system service to: (a) Deliver the system, component, or service
SA-4(5)	System, Component, and Service Configurations	for purpose" and meet the enterprise's requirements, whether purchasing directly from the OEM, channel partners, or a secondary market.	Functional	Equal	Configurations	TDA-02.4	(2) Use the pre-established, secure configuration as the default for any subsequent system, component, or service reinstallation or upgrade.	10	with [Assignment: organization-defined security configurations] implemented; and (b) Use the configurations as the default for any



Secure Controls Framework (SCF) 17 of 23

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM	STRM	SCF Control	SCF#	Secure Controls Framework (SCF)	Strength of Relationship	Notes (optional)
		NIST SP 800-161 R1 Supplemental C-SCRM Guidance	Rationale	Relationship			Control Description  Mechanisms exist to limit the use of commercially-provided Information	/ontional\	(a) Limit the use of commercially provided
SA-4(7)	Acquisition Process   NIAP-approved Protection Profiles	This control enhancement requires that the enterprise build, procure, and/or use U.S. Government protection profile-certified information assurance (A) components when possible. NIAP certification can be achieved for OTS (COTS and GOTS)	Functional	Intersects With	Information Assurance Enabled Products	TDA-02.2	Assurance (M) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-approved.	5	information assurance and information assurance-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-
SA-4(8)	Acquisition Process   Continuous Monitoring Plan for Controls	This control enhancement is relevant to C-SCRM and plans for continuous monitoring of control effectiveness and should therefore be extended to supplies, developers, system integrators, external system service providers, and other ICI/OT-related service providers.	Functional	Equal	Continuous Monitoring Plan	TDA-09.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a plan for the continuous monitoring of cybersecurity and data protection control effectiveness.	10	approved Protection Profile for a specific Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the organization.
SA-5	System Documentation	Information system documentation should include relevant C-SCRM concerns (e.g., C-SCRM plan). Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity.	Functional	Intersects With	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and for Services (TAAS) that describe:  (1) Secure configuration, installation and operation of the TAAS;  (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative	5	Obtain or develop administrator documentation for the system, system component, or system service that describes:     Secure configuration, installation, and operation of the system, component, or service;     Effective use and maintenance of security and orivacy functions and mechanisms: and
SA-5	System Documentation	Information system documentation should include relevant C-SCRM concerns (e.g., C-SCRM plan). Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity.	Functional	Intersects With	Asset Scope Classification	AST-04.1	is a unisidement functions.  Mechanisms exist to determine cybersecurity and data protection control applicability by identifying, assigning and documenting the appropriate assets cope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	5	orwacy uncuous and mechanisms; and a. Obtain of develop administrator documentation for the system, system component, or system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security and privacy functions and mechanisms; and
SA-8	Security and Privacy Engineering Principles	The following security engineering techniques are helpful for managing cybersecurity risks throughout the supply chain.  Anticipate the maximum possible ways that the ICT/OT product or service can be misused or abused in order to help identify how to protect the product or system from such uses. Address intended and unintended use scenarios in architecture and design.  D. Design network and security architectures, systems, and components based on the enterprise's risk botternoc as determined by risk assessments (see Section 2 and Anoendix CA.)	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 (TAS) that are consistent with industry-accepted system hardening standards.	5	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components. (Assignment or sganization-defined systems security and privacy engineering principles).
SA-8	Security and Privacy Engineering Principles	The following security engineering techniques are helpful for managing cybersecurity risks throughout the supply chain.  a. Anticipate the maximum possible ways that the ICT/OT product or service can be misused or abused in order to help identify how to protect the product or system from such uses. Address intended and unintended use scenarios in artificiation and design and the service of	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: (Assignment or oganization-defined systems security and privacy engineering principles).
SA-9	External System Services	C-SCRM supplemental guidance is provided in the control enhancements.	Functional	Equal	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	10	a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls];     b. Define and document organizational oversight
SA-9(1)	External System Services   Risk Assessments and Organizational Approvals	See Appendices C and D. Departments and agencies should refer to Appendix E and Appendix F to implement guidance in accordance with Executive Order 14028 on improving the Nation's Cybersecurity	Functional	Equal	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	10	and user roles and responsibilities with regard to (a) Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and (b) Verify that the acquisition or outsourcing of dedicated information security services is approved by (Assignment: organization-defined
SA-9(3)	External System Services   Establish and Maintain Trust Relationship with Providers	Relationships with providers should meet the following supply chain security requirements:  a. The requirements definition is complete and reviewed for accuracy and completeness, including the assignment of criticality to various components and defining operational concepts and associated scenarios for intended and unintended use.  b. Requirements are based on needs, relevant compliance drivers, criticality analysis, and assessments of opherasceutry risks throughout the supply chain.  C. Other supply chain threats, vulnerabilities, and associated risks are identified and documented.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposated Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	personnel or roles1. Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: (Basignmeth: organization- defined security and privacy requirements, properties, factors, or conditions defining accedable trust relationships1.
SA-9(3)	External System Services   Establish and Maintain Trust Relationship with Providers	Relationships with providers should meet the following supply chain security requirements:  A The requirements definition is complete and reviewed for excuracy and completeness, including the assignment of criticality to various components and defining operational concepts and associated scenarios for intended and unintended use.  N. Requirements are based on needs, relevant compliance drivers, criticality analysis, and assessments of opherascurity risks throughout the supply chain.  C. O'per supply host intrests, vulnerabilities, and associated risks are identified and documented.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Techniqoy Assets, Applications and/or Services (TAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization- defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].
SA-9(3)	External System Services   Establish and Maintain Trust Relationship with Providers	Relationships with providers should meet the following supply chain security requirements:  In Ter equirements definition is complete and reviewed for excuracy and completeness, including the assignment of criticality to various components and defining operational concepts and associated scenarios for intended and unintended use.  N. Requirements are based on needs, relevant compliance drivers, criticality analysis, and assessments of cybersecurity risks throughout the supply chain.  C. Octer supply chain threats, vulnerabilities, and associated risks are identified and documented.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to:  (I) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and  (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	Establish, document, and maintain trust retationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization- defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships1.
SA-9(3)	External System Services   Establish and Maintain Trust Relationship with Providers	Relationships with providers should meet the following supply chain security requirements.  In re-requirements definition is complete and reviewed for accuracy and completeness, including the assignment of criticality to various components and defining operational correpts and associated scenarios for intended and unintended use.  De Requirements are based on needs, relevant compliance drivers, criticality analysis, and assessments of opherascurity risks throughout the supply chain.  C. Ober supply chain threats, vulnerabilities, and associated risks are identified and documented.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization- defined security and privacy requirements, properties, factors, or conditions defining acceptable frust relationships!
SA-9(3)	External System Services   Establish and Maintain Trust Relationship with Providers	Relationships with providers should meet the following supply chain security requirements:  In Ter equirements definition is complete and reviewed for excuracy and completeness, including the assignment of criticality to various components and defining operational concepts and associated scenarios for intended and unintended use.  N. Requirements are based on needs, relevant compliance drivers, criticality analysis, and assessments of cybersecurity risks throughout the supply chain.  C. Octer supply chain threats, vulnerabilities, and associated risks are identified and documented.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisme exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	5	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization- defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].
SA-9(3)	External System Services   Establish and Maintain Trust Relationship with Providers	Relationships with providers should meet the following supply chain security requirements:  A The requirement definition is complete and reviewed for excuracy and completeness, including the assignment of criticality to various components and defining operational corriepts and associated scenarios for intended and unintended use.  N. Requirements are based on needs, relevant compliance drivers, criticality analysis, and assessments of opheraseculty risks throughout the supply chain.  C. O'ber supply with threats, vulnerabilities, and associated risks are identified and documented.	Functional	Intersects With	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurily and for data privacy controls.	5	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization- defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships1.
SA-9(4)	External System Services   Consistent Interests of Consumers and Providers	In the context of this enhancement, "providers" may include suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Equal	Conflict of Interests	TPM-04.3	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	10	Take the following actions to verify that the interests of [Assignment: organization-defined external service providers] are consistent with and reflect organizational interests: [Assignment organization-defined actions].
SA-9(5)	External System Services   Processing, Storage, and Service Location	The location may be under the control of the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Enterprises should assess C-SCRM risks associated with a given geographic location and apply an appropriate risk response, which may include defining bocations that are or are not acceptable and ensuring that appropriate protections are in place to address associated C-SCRM risk.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	Restrict the location of [Selection (one or more): information processing: information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].
SA-9(5)	External System Services   Processing, Storage, and Service Location	The location may be under the control of the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Enterprises should assess C-SCRM risks associated with a given geographic location and apply an appropriate risk response, which may include defining locations that are or are not acceptable and ensuring that appropriate protections are in place to address associated C-SCRM risk.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5	Restrict the location of (Selection (one or more): information processing; information or data; system services to (Assignment: organization-defined locations) based on (Assignment: organization-defined requirements or conditions).
SA-9(5)	External System Services   Processing, Storage, and Service Location	The location may be under the control of the suppliers, developers, system integrators, external system service providers, and other ICT/DT-related service providers. Enterprises should assess C-SCRM risks associated with a given geographic location and apply an appropriate risk response, which may include defining locations that are or are not acceptable and ensuring that appropriate protections are in place to address associated C-SCRM risk.	Functional	Intersects With	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physicial and virtual), infrastructure, systems components and/or shared with other third-parties.	5	Restrict the location of [Selection (one or more): information processing, information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].
SA-10	Developer Configuration Management	Developer configuration management is critical for reducing cybersecurity risks throughout the supply chain. By conducting configuration management activities, developers reduce the occurrence and itsellhood of these within increasing accountability and owneship for the change. Developer configuration management should be performed both by developers internal to federal agencies and integration or external service providers. Departments and agencies should refer to Appendix Fo implement this guidance in accordance with Executive Order 1420s, Improving the Nation's Cybersecurity.	Functional	Equal	Developer Configuration Management	TDA-14	Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation.	10	Require the developer of the system, system component, or system service to:  a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal]:  b. Document, manage, and control the integrity
SA-11	Developer Testing and Evaluation	Depending on the origins of components, this control may be implemented differently. For OTS (off-the-shell) components, the experient endual conduct research (e.g., who publicly available research (e.g., who publicly available resources) or request product determine whether the supplier (DBM) has performed such testing as part of their quality or scurity processes. When the exquirer has control over the application and development processes, they should require this testing as part of the SDLC. In addition to the specific types of resting activities described in the value of the straining or t	Functional	Equal	Cybersecurity & Data Protection Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybernecurity and data protection personnel to: (I) Create and implement a Sociary freeing and Enalusation (ST&E) plan, or (Z) implement a verifiable flam remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation moness and. Mechanisms exist to develop applications based on Sociary Software	10	b. bocument, manage, and control the internity Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to: a. Develop and implement a plan for ongoing security and privacy control assessments; b. Perform [Selection (one or more): unit; linteration: system: regression! a. Require the developer of the system, system
SA-15	Development Process, Standards, and Tools	revokuning occumente and romalized orevelopment processor so goal memas and system misigator developers is critical to the enterprise's efforts to effectively mitigate cybersecurity risks throughout the supply chain. The enterprise should apply national and international standards and best practices when implementing filts control. Using existing standards promotes consistency of implementation, reliable and defendable processes, and interoperability. The enterprise's development, maintenance, test, and deployment environments should all be oversed by this control. The tools included in this control can be manual or automated. The use of automated tools sids thoroughness, efficiency, and the scale of analysis	Functional	Equal	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	s. Neguine the developer of the systems, system component, or system service to follow a documented development process that:     1. Explicitly addresses security and privacy requirements:     2. Identifies the standards and tools used in the development process:



Secure Controls Framework (SCF) 18 of 23

FDE#	FDE Name	Focal Document Etement (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 (optional)
		Mot of 500-101 KT Supplemental Crocker Guidance	- reductate	netationship			Mechanisms exist to require the developer of the system, system component or service to perform a criticality analysis at organization-	Inntionall	Require the developer of the system, system component, or system service to perform a
SA-15(3)	Development Process, Standards, and Tools   Criticality Analysis	This enhancement identifies critical components within the information system, which will help determine the specific C-SCRM activities to be implemented for critical components. See C-SCRM Criticality Analysis described in Appendix C for additional context.	Functional	Equal	Criticality Analysis	TDA-06.1	defined decision points in the Secure Development Life Cycle (SDLC).	10	criticality analysis:  (a) At the following decision points in the system development life cycle: [Assignment: organization-defined decision points in the system development life cycle1: and
SA-15(4)	Development Process, Standards, and Tools   Threat Modeling and Vulnerability Analysis	This enhancement provides threat modeling and vulnerability analysis for the relevant federal agency and contractor products, applications, information systems, and networks. Performing this analysis will help integrate C.SCRM intro code refinement and modification activities. See the C-SCRM threat and vulnerability analyses described in Appendix C for additional context.	Functional	Equal	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	10	This control that exists within NIST SP 800-161 R1 was withdrawn from NIST 800-53 R5 and no longer exists.
SA-15(8)	Development Process, Standards, and Tools   Reuse of Threat and Vulnerability Information	In this enhancement encourages developers to reuse the threat and vulnerability information produced by prior development efforts and lessons learned from using the tools to inform origining development efforts. Doing so will help determine the C-SCRM activities described in Section 2 and Appendix C.	Functional	Equal	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	10	Require the developer of the system, system component, or system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.
SA-16	Developer-provided Training	Developer-provided training for external and internal developers is critical to C-SCRM. It addresses training the individuals responsible for federal systems and networks to include applicable development environments. Developer-provided training in this control solo applies to the individuals who select system and network components. Developer-provided training should include CSCRM materials to ensure that 1) developers are solved or potential threshes and vulnerabilities when developing, testing, and maintaining hardware and software, and 2) the individuals responsible for selecting system and network components. Developer training found also cover training for	Functional	Equal	Developer-Provided Training	TDA-16	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to provide training on the correct use and operation of the Technology Asset, Application and/or Service (TAAS).	10	Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: (Assignment organization-defined training).
SA-17	Developer Security and Privacy Architecture and Design	This control facilitates the use of C-SCRM information to influence system architecture, design, and component selection decisions, including security functions. Examples include identifying components that compose system architecture and design or selecting specific components to ensure swallability through multiple supplier or component selections. Departments and agencies should refer to Appendix To implement this guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity	Functional	Equal	Developer Architecture & Design	TDA-05	Nechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that: (1) is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; 2). Accurately and completely describes the remained security functionality.	10	Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that: a. is consistent with the organization's security and privacy architecture that is an integral part the organization's enterorise architecture:
SA-20	Customized Development of Critical Components	The enterprise may decide, based on their assessments of cybersecurity risks throughout the supply chain, that they require customized development of certain critical components. This control provides additional guidance on this activity. Enterprises should now with supplies and partners to ensure that critical components are identified. Organizations should ensure that they have a continued ability to maintain custom-developed critical software components. For example, beinging the source code, build scripts, and tests for a software component could enable an organization to have someone else maintain it if necessary.	Functional	Equal	Customized  Development of Critical  Components	TDA-12	Mechanisms exist to custom-develop critical system components, when Commercial Off The Shelf (COTS) solutions are unavailable.	10	Reimplement or custom develop the following critical system components: [Assignment: organization-defined critical system components].
SA-21	Developer Screening	The enterprise should implement screening processes for their internal developers. For system integrators who may be providing key developers that address official components, the enterprise should ensure that appropriate processes for developer receining flave bean used. The screening of developers should be received to the contract of the contrac	Functional	Equal	Developer Screening	TDA-13	Mechanisms exist to ensure that the developers of Technology Assets, Applications and/or Services (TAAS) have the requisite skillset and appropriate access authorizations.	10	Require that the developer of [Assignment: organization-defined system, system component, or system service]:  a. Has appropriate access authorizations as determined by assigned [Assignment: organization-defined official government duties]: and
SA-21(1)	Developer Screening   Validation of Screening	internal developer screening should be validated. Enterprises may validate system integrator developer screening by requesting summary data from the system integrator to be provided post-validation.	Functional	Intersects With	Developer Screening	TDA-13	Mechanisms exist to ensure that the developers of Technology Assets, Applications and/or Services (TAAS) have the requisite skillset and appropriate access authorizations.	5	This control that exists within NIST SP 800-161 R1 was withdrawn from NIST 800-53 R5 and no longer exists.
SA-22	Unsupported System Components	Acquiring products directly from qualified original equipment manufactures (CEHs) or their authorized distributions and resulters reduced spensoruly risks in the supply chain. The case of unsupported system components, the enterprise should use authorized resellers or distributors with an applicing it estationably with the supplier of the unsupported system components. When pruchasing alternative sources for continued support, enterprises should acquire directly from wetter diriginal equipment manufactures (CDHs) or their substituted distributions and resellers. Decisions about using alternative sources require input from the setternize's another information of the continued or setternize in a set of the continued or setternize in the continued or setternize is audinerized resources researched the differences in alternative commonstructures (CDHs) or their authorized.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAKS) by: (1) Removing and/or replacing TAKS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justicion and documented approval for the continued use of unsupported TAKS required to satisfy mission/business needs.	5	a. Replace system components when support for the components is no longer available from the developer, wendor, or manufacturer or b. Provide the following options for alternative sources for continued support for unsupported components [Selection (nee or more): in-house support: [Assignment: orsanization-defined a. Replace system components when support for
SA-22	Unsupported System Components	estimates and reselves reduces openescivity risks in the supply chain. In the case of unsupported system components, the enterprise should use authorised reselves or distributions with an ongoing relationship with the supplier of the unsupported system components. When purchasing alternative sources for continued support, enterprises about account develop from vetted original explanement analysis of the support, enterprises about account develop from vetted original explanement analysis careful support, enterprises about account develop from the development of supports. The support of	Functional	Intersects With	Alternate Sources for Continued Support	TDA-17.1	Mechanisms exist to provide in-house support or contract external providers for support with unsupported Technology Assets, Applications and/or Services (TAAS).	5	the components is no longer available from the developer, vendor, or manufacturer, or b. Provide the following options for attensative sources for continued support for unsupported components [Selection (one or more): in-house support [Assignment: organization-defined
SC-1	Policy and Procedures	System and communications protection policies and procedures should address ophersecurity risks throughout the supply chain in relation to the enterprise's processes, systems, and networks. Enterprise-level and program-specific policies help establish and clarify these requirements, and corresponding procedures provide instructions for meeting these requirements. Policies and procedures should include the coordination of communications among and across multiple enterprise entitles within the enterprise, as well as the communications methods, determine connections, and processes used between the enterprise and its	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	a. Develop, document, and disseminate to (Assignment: organization-defined personnel or roles): 1. [Selection (one or more): Organization-level; Mission/Dusiness process-level; System-level) system and communications protection policy that:
SC-1	Policy and Procedures	succliers, developers, existen integrations, external system sectories providers, and other (TOT-related System and communications protection proficies and procedures should address objectsecountly risks throughout the supply chain in relation to the enterprise's processes, systems, and networks. Enterprise-level and program-specific posities help establish and clarify these requirements, and corresponding process provide instructions for meeting these requirements. Policies and procedures should include the supplications of the process of the process of the processes of the processes and the succonfination of communications among and cross multiple enterprise entities within the enterprise, as well as the communications mentods, external connections, and processes used between the enterprise and its succliers, developers, sustem integrations, certain systems enterprise convictions, and force (crossing on direct (TOT)-related mentods of the processes o	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:     [Selection (one or more): Organization-level; Mission/Rusiness process-level; System-level] system and communications protection policy
SC-1	Policy and Procedures	System and communications protection policies and procedures should address cybersecurity risks throughout the supply chain in relation to the enterprise's processes, systems, and rebrooks. Enterprise-level and program-specific policies help establish and clarify these requirements, and corresponding procedures provide instructions for meeting these requirements. Policies and procedures should include the coordination of communications among and across muttiple enterprise entities within the enterprise, as well as the communications meethods, external connections, and processes used between the enterprise and its supplies. Swellow process. Swellam interactions, contrast system envire provide provide professional process.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:     1. [Selection (one or more): Organization-level; Mission/Dusiness process-level; System-level] system and communications protection policy that:
SC-1	Policy and Procedures	System and communications protection policies and procedures should address ophersecurity risks thoughout the supply chain in relation to the enterprise's processes, systems, and networks. Enterprise-level and program-specific policies help establish and clarify these requirements, and corresponding procedures prodice instructions for meeting these requirements. Policies and procedures should include the coordination of communications among and across multiple enterprise entitles within the enterprise, as well as the communications methods, determine connections, and processes used between the enterprise and its	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, 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; hission/Dusiness process-level; System-level] system and communications protection policy that:
SC-4	Information in Shared System Resources	spooliers, developers, existent integrations, external system service providers, and other ICT/OT-netated The enterprise may have information system resources with system suppliers, developers, system integrations, external system service providers, and other ICT/OT-related service providers. Protecting information in shared resources in support of various supply of hims activative is challenging when outsourcing key operations. Enterprises may either share too much and increase their risk or share too little and make it difficult for suppliers, developers, system integrators, external system service providers, and other ICT/OT related service providers to be efficient in their service delivery. The enterprise should work with developers define a structure or process for information sharing, includint the data shared, the method of sharing, and to	Functional	Equal	Information In Shared Resources	SEA-05	Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.	10	Prevent unauthorized and unintended information transfer via shared system resources.
SC-5	Denial-of-service Protection	C-SCRM Guidance supplemental guidance is provided in control enhancement SC-5 (2).	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	a. (Selection: Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; and b. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of- service objective: [Assignment]
SC-5(2)	Denial-of-service Protection   Capacity, Bandwidth, and Redundancy	The enterprise should include requirements for excess capacity, bandwidth, and redundancy into agreements with suppliers, developers, system integrators, external system service providers, and other KCT/OT-related service providers.	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.
SC-5(2)	Denial-of-service Protection   Capacity, Bandwidth, and Redundancy	The enterprise should include requirements for excess capacity, bandwidth, and redundancy into agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.	Functional	Intersects With	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	5	Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.
SC-7	Boundary Protection	The enterprise should implement appropriate monitoring mechanisms and processes at the boundaries between the agency systems and suppliers, developers, system integrators, external system service providers, and other ICIOT-related service providers' systems. Provisions for boundary protections should be incorporated into agreements with suppliers, developers, system integrators, external systems service providers, and other ICIOT-related service providers. There may be multiple interfaces throughout the exterprise, supplier systems and networks, and the SDLC. Appropriate vulnerability, threat, and risk	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;     Implement subnetworks for publicly accessible system components that are
SC-7(13)	Boundary Protection   Isolation of Security Tools, Mechanisms, and Support Components	assessments should be enformed to ensure cooper foundary extenctions for supply chain commonents and the enterprise should provide separation and isolation of development, test, and society assessment tools and operational environments and relevant monitoring tools within the enterprise's information systems and retworks. This control applies the entity responsible for creating software and hardware, to include federal agencies and prime contractors. As such, this controls applies to the federal agency and applicibate supplies information systems and networks. Enterprises should require their prime contractors to implement the control and flow down this requirement to relevant sub-lier contractors. If a compromise or information stands are based on an one environment, the other environments should still be notested through the skakes based on an one environment.	Functional	Intersects With	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.	5	ISelection: physically: obscally! separated from Isolate [Assignment: organization-defined information security tools, mechanisms, and support components] from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.
SC-7(14)	Boundary Protection   Protect Against Unauthorized Physical Connections	This control is relevant to C-SCRM as it applies to external service providers.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces].



ecure Controls Framework (SCF) 19 of 23

FDE#	FDE Name	Focal Document Element (FDE) Description NIST SP 800-161 R1 Supplemental C-SCRN Guidance	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
	Boundary Protection I						Physical access control mechanisms exist to protect system components from unauthorized physical access (e.g., lockable physical casings).	iontional	
SC-7(14)	Boundary Protection   Protect Against Unauthorized Physical Connections	This control is relevant to C-SCRM as it applies to external service providers.	Functional	Intersects With	Lockable Physical Casings	PES-03.2	, , , , , , , , , , , , , , , , , , , ,	5	Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces].
SC-7(14)	Boundary Protection   Protect Against Unauthorized Physical Connections	This control is relevant to C-SCRM as it applies to external service providers.	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces].
SC-7(19)	Boundary Protection   Block Communication from Non- organizationally Configured Hosts	This control is relevant to C-SCRM as it applies to external service providers.	Functional	Intersects With	Network Access Control (NAC)	AST-02.5	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	5	Block inbound and outbound communications traffic between [Assignment: organization- defined communication clients] that are independently configured by end users and external service providers.
SC-8	Transmission Confidentiality and Integrity	The requirements for transmission confidentiality and integrity should be integrated into agreements with suppliers, developers, system integrations, external system service providers, and other ICTIOT-related service providers. Acquirers, suppliers, developers, system integrations, centernal system service providers, and other ICTIOT-related service providers may repurpose existing security mechanisms (e.g., and autherications, authorization, or encryption) to achieve enterprise confidentiality and integrity requirements. The degree of protection should be based on the sensitivity of information to be transmitted and the relationship between the enterprise and the suppliers, developers, system integrators, external system systems and the systems of the suppliers of the systems of th	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.
SC-8	Transmission Confidentiality and Integrity	The equirements for transmission confidentiality and integrity should be integrated into agreements with suppliers, developers, system integration, external system service providers, and other ICTOT-related service providers. Acquirers, suppliers, evelopers, system integrations, caternal system service providers, and other ICTOT-related service providers may repurpose existing security mechanisms (e.g., authoritication, submixiation, or encypholion) to achieve enterprise confidentiality and integrity requirements. The degree of protection should be based on the sensitivity of information to be transmitted and the relationship between the enterprise and the suppliers, developers, system interprises, external system systems.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	Protect the [Selection (one or more): confidentiality; integrity) of transmitted information.
SC-18	Transmission Confidentiality and Integrity	The enterprise should use this control in various applications of mobile code within their information systems and networks. Examples include acquisition processes such as the electronic transmission of supply chain information (e.g. entail), the receipt of software components, logistics information management in RFID, or transport sensors infrastructure.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system- independent applications.	5	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.
SC-18(2)	Mobile Code   Acquisition, Development, and Use	he enterpoise should employ rigorous supply chain protection techniques in the acquisition, development, and use of mobile code to be deployed in the information system. Examples include ensuing that mobile odde originates from vetted sources when acquise, that vetted system integrators are used for the development of custom mobile code or prior to installing, and that vetification processes are in place for acceptance criteria prior to installiation in order to verify the source and integrity of code. Note that mobile code can be both order for the underlying information systems and networks (e.g., PRI device applications)	Functional	Intersects With	Software Licensing Restrictions	AST-02.7	Mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions.	5	Verify that the acquisition, development, and use of mobile code to be deployed in the system meets [Assignment: organization-defined mobile code requirements].
SC-18(2)	Mobile Code   Acquisition, Development, and Use	or for information externs and components.  The enterprise should employ rigious supply thain protection techniques in the acquisition, development, and use of mobile code to be deployed in the information system. Examples include ensuring that mobile code originates from weter doucree when acquired, that veter depression are used for the development of custom mobile code or prior to installing, and that verification processes are in place for acceptance entering prior to installation in order to verify the source and mitergity of code. Note that mobile code can be obtor close for the underlying information systems and networks (e.g., RFID device applications)	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system- independent applications.	5	Verify that the acquisition, development, and use of mobile code to be deployed in the system meets [Assignment: organization-defined mobile code requirements].
SC-27	Platform-independent Applications	or for information avatems and components.  The use of trusted platform-independent applications is essential to CSCRM. The enhanced portability of platform-independent applications enables enterprises to availth externs is service providers more readily in the event that one becomes compromised, hereby reducing vendor-dependent oppresently risks. This is especially relevant for critical applications on which multiple systems may rely	Functional	Equal	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system- independent applications.	10	Include within organizational systems the following platform independent applications: [Assignment: organization-defined platform-independent applications].
SC-28	Protection of Information at Rest	The enterprise should include provisions for the protection of information at rest into their agreements with suppliers, developers, system integration, external system service providers, and other ICT/IOT-leated service providers. The enterprise should also ensure that they provide appropriate protections within their softward providers and networks for data at rest for the suppliers, developers, system integrations, external system service providers, and other IOT-Presteded service providers information, such as source code, testing data, blue-prints, and intellectual property information. This control should be applied throughout the SOC L; including during requirements, development, manufacting, test, inventory management,	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	Protect the [Selection (one or more): confidentiality; integrity) of the following information at rest: [Assignment: organization- defined information at rest].
SC-28	Protection of Information at Rest	The enterprise should include provisions for the protection of information at rest into their agreements with suppliers, developers, system integrators, external system service providers, and their (IZFOT-related service providers. The enterprise should also ensure that they provide appropriate protections within the information systems and networks for data are let for the suppliers, developers, system integrators, ceternal system service providers, and other ICFOT-related service providers information, such as source code, testing data, bulgerins, and intellectual property information. This control should be applied throughout the	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization- defined information at rest].
SC-29	Heterogeneity	SIC. Including during requirements, development, manufacturins, test, investor management. Heterogeneity lectriques include the use of different operating systems, virtualization techniques, and multiple sources of supply. Multiple sources of supply can improve component availability and reduce the impact of a supply often jordersecurity components. In case of a supply chain inspressecurity compromises, an attemative source of supply will allow the enterprises to more rapidly existin to an atternative system/component that may not be affected by the compromise. Additionally, heterogeneous components decrease the attack surface by limiting the impact to the subset of the infrastructure that is using vulnerable	Functional	Equal	Heterogeneity	SEA-13	Mechanisms exist to utilize a diverse set of technologies for system components to reduce the impact of technical vulnerabilities from the same Original Equipment Manufacturer (OEM).	10	Employ a diverse set of information technologies for the following system components in the implementation of the system: [Assignment: organization-defined system components].
SC-30	Concealment and Misdirection	commonenes.  Concealment and misdirection techniques for C-SCRM include the establishment of random resupply times, the concealment of location, randomly changing the fake location used, and randomly changing or shifting information storage into alternative servers or storage mechanisms.	Functional	Intersects With	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for systems to confuse and mislead adversaries.	5	Employ the following concealment and misdirection techniques for [Assignment: organization-defined systems] at [Assignment: organization-defined time periods] to confuse and mislead adversaries: [Assignment: organization-defined concealment and misdirection techniques].
SC-30(2)	Concealment and Misdirection   Randomness	Supply chain processes are necessarily structured with predictable, measurable, and repeatable processes for the purpose of efficiency and cost reduction. This opens up the opportunity for potential breach, in order to restor the processor of the purpose of efficiency and costs in other costs of the processor o	Functional	Equal	Randomness	SEA-14.1	Automated mechanisms exist to introduce randomness into organizational operations and assets.	10	Employ [Assignment: organization-defined techniques] to introduce randomness into organizational operations and assets.
SC-30(3)	Concealment and Misdirection   Change Processing and Storage Locations	Changes in processing or storage locations can be used to protect downloads, deliveries, or associated supply chain metadata. The enterprise may leverage such techniques within the their information systems and networks to create uncertainty about the activities targeted by adversaries. Establishing a few process changes and randomling their use -whether it is for receiving, acceptance testing, storage, or other supply chain activities - can aid in reducing the likelihood of a supply chain event.	Functional	Equal	Change Processing & Storage Locations	SEA-14.2	Automated mechanisms exist to change the location of processing and/or storage at random time intervals.	10	Change the location of [Assignment: organization- defined processing and/or storage] [Selection: [Assignment: organization-defined time frequency]: at random time intervals]].
SC-30(4)	Concealment and Misdirection   Misleading Information	The enterprise can convey misleading information as part of concealment and misdirection efforts to protect the information system being developed and the enterprise's systems and networks. Examples of such efforts in security include homeynets or virtualized environments. Interprise developed to convey misleading information. These may be considered advanced techniques that require experienced resources to effectively implement them. If an enterprise decides to use honeypots, it should be done in concert with legal conusels of following the enterprise's policies.	Functional	Intersects With	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for systems to confuse and mislead adversaries.	5	Employ realistic, but misleading information in [Assignment: organization-defined system components] about its security state or posture.
SC-30(5)	Concealment and Misdirection   Concealment of System Components	The enterprise may employ various concealment and misdirection techniques to protect information about the information system being developed and the enterprise's information systems and networks. For example, the delivery of critical components to a central or trusted third-party deplor can be used to conceal or misdirect any information regarding the component is use or the enterprise using the component. Separating components from their associated information in differing physical and electronic delivery channels and obfuscating the information through various techniques can be used to conceal information through various techniques can be used to conceal information throughout the component or its use, condition, or other	Functional	Intersects With	Concestment & Misdirection	SEA-14	Mechanisms exist to utilize concesiment and misdirection techniques for systems to confuse and mislead adversaries.	5	Employ the following techniques to hide or conceal (Assignment: organization-defined system components): [Assignment: organization- defined techniques].
SC-36	Distributed Processing and Storage	Processing and storage can be distributed both across the enterprise's systems and networks and across the SDC. The enterprise should ensure that these techniques are applied in both contexts. Development, manufacturing, configuration management, east, maintenance, and operations can use distributed processing and storage. This control applies to the entity responsible for processing and storage functions or related infrastructure, to include federal agencies and controlsor. As such, this control applies to the federal agency and applicable supplier information systems and networks. Enterprises should require their prime contractors to innolement this accrotic and flow down this resolution extrement to related the liter contractors.	Functional	Equal	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.	10	Distribute the following processing and storage components across multiple [Selection: physical locations; logical domains]: [Assignment: organization-defined processing and storage components].
SC-37	Out-of-band Channels	C-SCRM-specific supplemental guidance is provided in control enhancement SC-37 (1).	Functional	Intersects With	Out-of-Band Channels	NET-11	Mechanisms exist to utilize out-of-band channels for the electronic transmission of information and/or the physical shipment of system components or devices to authorized individuals.	5	Employ the following out-of-band channels for the physical delivery or electronic transmission of [Assignment: organization-defined information, system components, or devices] to [Assignment: organization-defined individuals or systems]: [Assignment: organization-defined out- of-band channels].
SC-37(1)	Out-of-band Channels   Ensure Delivery and Transmission	The enterprise should employ security safeguards to ensure that only specific individuals or information systems receive the information about the information system or its development environment and processes. For example, proper credentisting and authorization documents should be requested and verified prior to the release of critical components, such as custom chips, custom software, or information during delivery.	Functional	Intersects With	Out-of-Band Channels	NET-11	Mechanisms exist to utilize out-of-band channels for the electronic transmission of information and/or the physical shipment of system components or devices to authorized individuals.	5	on-band channels). Employ (Assignment: organization-defined Employ (Assignment: organization-defined controls) to ensure that only (Assignment: organization-defined individuals or systems) receive the following information, system components, or devices: (Assignment: organization-defined information, system components, or devices!
							Mechanisms exist to establish and maintain a Security Operations Center (SOC) that facilitates a 24x7 response capability.		Employ the following operations security controls
SC-38	Operations Security	The enterprise should ensure that appropriate supply chain threat and vulnerability information is obtained from and provided to the applicable operational security processes.	Functional	Intersects With	Security Operations Center (SOC)	OPS-04		5	to protect key organizational information throughout the system development life cycle: [Assignment: organization-defined operations security controls].



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 (optional)
SC-38	Operations Security	The enterprise should ensure that appropriate supply chain threat and valnerability information is obtained from and provided to the applicable operational security processes.	Functional	Intersects With	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	5	Employ the following operations security controls to protect key organizational information throughout the system development life cycle: [Assignment organization-defined operations security controls].
SC-47	Alternate Communications Channels	If necessary and appropriate, suppliers, developers, system integrators, external system service providers, and other ICTOT-related service providers should be included in the alternative communication paths described in this control.	Functional	Equal	Alternate Communications Channels	BCD-10.4	Mechanisms exist to maintain command and control capabilities via alternate communications channels and designating alternative decision makers if primary decision makers are unavailable.	10	Establish [Assignment: organization-defined alternate communications paths] for system operations organizational command and control.
SI-1	Policy and Procedures	The enterprise should include C-SCRM in system and information integrity policy and procedures, including ensuring that program-specific requirements for employing various integrity verification tools and techniques are clearly defined. System and information integrity for information systems, components, and the underlying information systems and networks is critical for managing cybersecurity risks throughout the supply chain. The insertion of malicious code and counterfeits are two primary examples of cybersecurity risks throughout the supply chain, both of which can be at least partially addressed by deploying system and	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:     1, Selection (one or more): Organization-level; Mission/business process-level; System-level; system and information integrity policy that:
Si-1	Policy and Procedures	information intestity controls.  The enterprise should include C-SCRM in system and information integrity policy and procedures, including ensuring that program-specific requirements for employing various integrity verification tools and techniques are clearly defined, System and information integrity for information systems, components, and the underlying information systems, components, and the underlying information systems and networks is critical for managing cybersecurity risks throughout the supply chain. The intention of mislicious code and counterfields are two primary seamples of cybersecurity risks throughout the supply chain, both of which can be at least partially addressed by deploying system and information integrity controls.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	fal Addresses ournose, scoes, roles.  a. Develop, document, and disseminate to [Assignment-organization-defined personnel or roles]:  [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that:
SI-1	Policy and Procedures	The interprise about fortubed C SCRM in system and information integrity policy and procedures, including enturing that program-specific requirements for employing valorics integrity vertication tools and techniques are clearly defined, system and information integrity for information systems, components, and the underlying information systems components, and the underlying information systems and networks is critical for managing cybersecurity risks throughout the supply chain. The interaction of misciscious code and counterfields are two primary seamples of cybersecurity risks throughout the supply chain, both of which can be at least partially addressed by deploying system and information interfield controls.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	(a) Addresses purpose, scope, roles, a. Develop, document, and disseminate to (Assignment: organization-defined personnel or roles): I, [Selection (one or more): Organization-level; Mission/Dusiness process-level; System-level] system and information integrity policy that: (a) Addresses purpose, scope, roles.
SI-2	Flaw Remediation	The output of flaw remediation activities provides useful input into the ICT/OT SCRM processes described in Section 2 and Appendix C. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	a. Identify, report, and correct system flaws; b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the
SI-2	Flaw Remediation	The output of flaw remediation activities provides useful input into the ICT/OT SCRM processes described in Section 2 and Appendix C. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	a. Identify, report, and correct system flaws;  D. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;  C. Install security-relevant software and firmware updates within [Assignment: organization-defined time period of the release of the
SI-2	Flaw Remediation	The output of flaw remediation activities provides useful input into the ICT/OT SCRM processes described in Section 2 and Appendix C. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Intersects With	Automatic Antimatware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	Identify, report, and correct system flaws;     D. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;     C. Install security-relevant software and firmware updates within [Assignment: organization-defined time period of the release of the
SI-2(5)	Flaw Remediation   Automatic Software and Firmware Updates	The enterpoise should specify the various software assets within its information systems and networks that require automated updates (both indirect and direct). This specification of assets should be defined from criticality analysis results, which provide information on critical and non-critical functions and components (see Section 2 and Appendix C). A centralized patch management process may be employed for evaluating and managing updates prior to deployment. Those software assets that require inforce updates from a supplier should only accept updates that originate directly from the OEN unless specifically deployed by the acquirer, such as with a centralized datch management process. Deservations and sense is should refer to Appendix P.	Functional	Intersects With	Automated Software & Firmware Updates	VPM-05.4	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.	5	Install [Assignment: organization-defined security-relevant software and firmware updates] automatically to [Assignment: organization-defined system components].
SI-3	Malicious Code Protection	Because the majority of code operated in federal systems is not developed by the Federal Government, maintious code threst often of simple time the supply chain. This controls applies to the federal agency and contractors with code-related responsibilities (e.g., developing code, installing patches, performing system upgrades, etc.), as well as applicable contractor information systems and networks. Enterprises should require their prime contractors to impelment this control and filow down this requirement to relevant sub-tier contractors. Departments and agencies should refor to Appendix Fi to implement this guidance in accordance with Executive Order 1428, Improving the Nation's Cybersocutive.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	a. Implement [Selection (one or more): signature based; non-signature based; malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational
SI-3	Malicious Code Protection	Because the majority of code operated in tederal systems is not developed by the Federal Government, malicious code threats often originate from the supply chain. This controls applies to the federal agency and contractors with code-lested responsibilities (e.g., developing code, installing patches, performing system upgrades, etc.), as well as applicable contractor information systems and networks. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-lier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Security of 4028. Improvint the Nation's Observacion.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	a. Implement [Selection (one or more): signature based; non-signature based molicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational
SI-3	Malicious Code Protection	with Executive Oxfert 18228. Immovives the Nation's Ochereacurity.  Because the majority or dod operated in federal systems in not developed by the Federal Government, malicious code threats often originate from the supply chain. This control applies to the federal agency and contractors with code-related repropriatibilities e.g., developing code, installing patches, performing system upgrades, etc.), as well as applicable contractors information systems and networks. Enterprises should sequile 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 Oxfert 4228. Improvint the Nation's Oxferts curity.	Functional	Intersects With	Malicious Code Protection (Anti- Malware)	END-04	Mechanisms exist to utilize antimatware technologies to detect and eradicate malicious code.	5	a. Implement [Selection (one or more): signature based; non-signature based malicious coduce brotection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational
SI-3	Malicious Code Protection	Secause the majority of code operated in federal systems is not developed by the Federal Government, malicious code threats often originate from the supply chain. This controls applies to the federal agency and contractors with code-related responsibilities (e.g., developing code, installing patches, performing system upgrades, etc.), as well as applicable contractor information systems and networks. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-lier contractors. Departments and agencies should refer to Appendix Fo implement this guidance in accordance with Securitive Order 14508. Improvint the Nation's Observacions.	Functional	Intersects With	Heuristic / Nonsignature Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimatware detection capabilities.	5	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational
SI-3	Malicious Code Protection	Because the majority of code operated in federal systems is not developed by the Federal Government, mailcious code threst often of general center supply chain. This controls applies to the federal agency and contractors with code-related responsibilities (e.g., developing code, installing patches, performing system upgrades, etc.), as well as applicable contractor information systems and networks. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. Despirement and agencies soludid refer to Appendix 6 to implement spidance in accordance	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocobs to safeguard sensitive/regulated data during transmission over open, public networks.	5	a. Implement (Selection (one or more): signature based; non-signature based; non-signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; D. Automatically update malicious code protection mechanisms as new releases are available in accordance with oreanizational.
SI-3	Malicious Code Protection	with Executive Order 14028. Improving the Nation's Ochersecutiv.  Because the majority of code operated in federal systems in a cit developed by the Federal Government, malicious code threats often originate from the supply chain. This control applies to the federal agency and contractors with code-related repropriatibilities e.g., developing code, installing patches, performing system sugrandes, etc.), as well as applicable contractor with contractors with contractors with contractors with contractors. Enterprises should require their prince contractors to implement this control and flow down this requirement to relevant sub-lier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance	Functional	Intersects With	Automatic Antimatware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are
SI-3	Malicious Code Protection	with Executive Order 14028. Improvine the Nation's Orbersecutiv.  Because the majority of code operated in federal systems in sort of eveloped by the Federal Government, malicious code threats often originate from the supply chain. This control applies to the federal agency and contractors with code-related responsibilities (e.g., developing code, installing patches, performing system rugardes, etc.), as well as applicable contractors information systems and networks. Enterprises should require their prime contractors to implement this control and flow down this recipitament to relevant sub-lier contractors. Departments and agencies should refer for Appendix Fo implement this guidance in accordance selfs. Executive Order 14028, Improving the Nation's Octobersecutive.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	available in accordance with organizational a. Implement [Selection (one ormor): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; D. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational
SI-4	System Monitoring	This control includes monitoring vulnerabilities that result from past supply chain opersecurity compromises, such a mallicious code implained during orbinare development and set to activate after deployment. System monitoring is frequently performed by external service providers. Service-level agreements with these providers should be entructured to apportulately reflect this control. Enterprises should require their prime contraction to implement this control and flow down this requirement to result with the prime contraction to implement this control and flow down this requirement to require the prime contraction to implement this control and flow down this requirement to result and the prime contraction to implement this control and the variety of the prime control and the prim	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]: and 2. Unauthorized local, network, and remote connections:
SI-4	System Monitoring	This control includes monitoring vulnerabilities that result from past supply chain cybersecurity compromises, such as millicious code implanted during software development and set to activate after deployment. System monitoring is frequently performed by external service providers. Service-level agreements with these providers should be structured to appropriately reflect this control. Enterprises should require their prime contractors to implement this control and fow down this requirement to relevant sub-tier contractors. Departments and agencies should refer to Appendix Fo implement this guidance in accordance with Security collect 4528. Improvive the Nation's Observacy.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security- related event logs.	5	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]: and 2. Unauthorized local, network, and remote connections:
SI-4	System Monitoring	This control includes monitoring vulnerabilities that result from past supply chain opersecurity compromises, such as malicious code implanted during software development and set to activate after deployment. System monitoring is frequently performed by external service providers. Service-level agreements with these providers should be structured to appropriately reflect this control. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-lier contractors. Departments and agencies should refer to Appendix Fo implement this guidance in accordance with Security of 1428. The morrow the Nation's Observacions.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]: and 2. Unauthorized local, network, and remote connections:
SI-4	System Monitoring	such securious users 14078, improved the Nation's Albertecutor.  This control includes emotioning vulnerabilities that result through ast supply chain cybersecutify compounties, such as malicious code implantate during software development and set to activate after deployment. System monitoring is frequently performed by external service providers. Service-level agreements with these providers should be structured to appropriately reflect this control. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-lier contractors. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Securitive Order 14028. Improvine the Nation's Chemisters.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	connections:  a. Monitor the system to detect:  1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]: and  2. Unauthorized local, network, and remote connections:
SI-4(17)	System Monitoring   Integrated Situational Awareness	System monitoring information may be correlated with that of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, if appropriate. The results of correlating monitoring information may point to supply chain cybersecurity vulnerabilities that require mitigation or compromises.	Functional	Equal	Integration of Scanning & Other Monitoring Information	MON-02.3	Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to surber enhance the ability to identify inappropriate or unusual activity.	10	Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.



cure Controls Framework (SCF) 21 of 23

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM	STRM	SCF Control	SCF#	Secure Controls Framework (SCF)	Strength of Relationship	Notes (optional)
		NIST SP 800-161 R1 Supplemental C-SCRM Guidance	Rationale	Relationship			Control Description  Mechanisms exist to implement enhanced activity monitoring for	Inntinnall	
SI-4(19)	System Monitoring   Risk for Individuals	Persons identified as being of higher risk may include enterprise employees, contractors, and other third parties (e.g., voluneers, visitors) who may have the need of shilly to access to an enterprise's system, network, or system environment. The enterprise may implement enhanced oversight of these higher-risk individuals in accordance with policies, procedures, and – if relevant – terms of an agreement and in coordination with appropriate officials.	Functional	Equal	Individuals Posing Greater Risk	MON-01.14	individuals who have been identified as posing an increased level of risk.	10	Implement [Assignment: organization-defined additional monitoring] of individuals who have been identified by [Assignment: organization-defined sources] as posing an increased level of risk.
SI-5	Security Alerts, Advisories, and Directives	The enterprise should evaluate security siters, advancines, and directives for cybersecurity supply chain impacts and follow by fineded. US-CERT, FASC, and other authoritative entities generate security siters and solvisories that are applicable to C-SCRN. Additional taws and regulations will impact who and how additional advisories are provided. Enterprises should ensure that their infirmation-sharing protocol and processes include sharing sterns, advisories, and directives with relevant parties with whom they have an agreement to deliver products or perform services. Enterprises should provide direction or guidance as to what actions.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;     b. Generate internal security alerts, advisories, and directives as deemed necessary;
SI-5	Security Alerts, Advisories, and Directives	to be taken in response to sharing such an alert, advisors, or directive. Enterprises should require their orime The enterprises should require deviated security superly, original impacts and follow up if needed, U.S-CERT, FASC, and other authoritative entities generate security slept and advisories that are applicable to S-CERT, Additional twas and reglustions will impact and hardward and advisories that are applicable to S-CERT, Additional twas and reglustions will impact with one and how processes include sharing slents, advisories, and directives with relevant parties with whom they have an agreement to additive products or perform services. Enterprises should provide direction or guidence as to what actions are deviately reported to perform services. Enterprises should provide direction or guidence as to what actions are	Functional	Intersects With	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of stracker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	c. Disseminate security alerts, advisories, and a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generate internal security alerts, advisories, and directives as deemed necessary;
SI-5	Security Alerts, Advisories, and Directives	to be taken in response to sharing such an alert, advisore, or directive. Enterprises should require their orine. The enterprises should evaluate security suelts, advisories, and directives for cyberaccurity supply, chain impacts and follow up if needed, US-CERT, FASCs, and other authoritative entities generate security alert and advisories that are applicable to US-CERT, Additional times and regulations will impact with on and how additional solvisories are provided. Enterprises should ensure that their information-sharing protocols and processes include sharing enters, advisories, and directives with relevant parties with whom they have an agreement to deliver products or perform services. Enterprises should provide direction or guidance as to what action are to be taken in response to sharing such an after, advisory, or directive. Enterprises should require their prime.	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	c. Disseminate security alerts, advisories, and a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generate internal security alerts, advisories, and directives as deemed necessary; c. Disseminate security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and
SI-7	Software, Firmware, and Information Integrity	This control applies to the federal agency and applicable supplier products, applications, information systems, and networks. The integrity of all applicable systems and networks should be systemstacilly tested and verified to ensure that it remains as required so that the systems/components traversing through the supply chain are not impacted by unanticipated changes. The integrity of systems and components should also be tested and verified. Applicable verification tools include glight signature or checksum verification; acceptance testing for physical components; confining software to limited privilege environments, such as anotholess: code execution in contained environments and to use and ensuring that I forbly binary or sentitives.	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FM), or similar technologies, to detect and report or unauthorized changes to selected files and configuration settings.	5	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information;] and b. Take the following actions when unauthorized changes to the software, firmware, and
SI-7	Software, Firmware, and Information Integrity	This control applies to the federal agency and applicable supplier products, applications, information systems, and networks. The integrity of all applicable systems and networks should be systemstically tested and verified to ensure that it remains as required so that the systems components traversing through the supply chain are not impacted by unanticipated changes. The integrity of systems and components should also be tested and writeful. Applicable verification tools include gliable signature or checksum verifications, acceptance testing for physical components; confining software to limited privilege environments, such as sandboxes: code execution in contrained environments in our use: and ensuring that I for thy binary or sandboxes: code execution in contrained environments in or to use: and ensuring that I for thy binary or sandboxes: code execution in contrained environments in or to use: and ensuring that I for thy binary or sandboxes: code execution in contrained environments or the use: and ensuring that I for thy binary or sandboxes: code execution in contrained environments or the sandboxes.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; and b. Take the following actions when unauthorized chances to the software. Firmware, and
SI-7	Software, Firmware, and Information Integrity	This control applies to the federal agency and applicable supplier products, applications, information systems, and networks. The integrity of all applicable systems and networks should be systemstacilly tested and verified to ensure that it remains as required so that the systems/components traversing through the supply chain are not impacted by unarticipated changes. The integrity of systems and components should also be tested and verified. Applicable verification tools include glight signature or checksum verification; acceptance testing for physical components; confining software to limited privilege environments, such as sandboxes: Code execution in containing environments in our use and ensuring that If only binary or sandboxes: Code execution in containing environments and to use and ensuring that If only binary or sandboxes: Code execution in containing environments.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information; and b. Take the following actions when unauthorized changes to the software. Firmware. and
SI-7(14)	Software, Firmware, and Information Integrity   Binary or Machine Executable Code	The enterprise should obtain binary or machine-executable code directly from the OEM/developer or other verified source.	Functional	Intersects With	Binary or Machine- Executable Code	END-06.7	Mechanisms exist to prohibit the use of binary or machine-executable code from sources with limited or no warranty and without access to source code.	5	This control that exists within NIST SP 800-161 R1 was withdrawn from NIST 800-53 R5 and no longer exists.
SI-7(15)	Software, Firmware, and Information Integrity   Code Authentication	The enterprise should ensure that code authentication mechanisms, such as digital signatures, are implemented to ensure the integrity of software, firmware, and information.	Functional	Intersects With	Signed Components	CHG-04.2	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.	5	Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [Assignment: organization-defined software or firmware components].
SI-12	Information Management and Retention	C-SCRM should be included in information management and retention requirements, especially when the sensitive and proprietary information of a system integrator, supplier, or external service provider is concerned.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	Manage and retain information within the system and information output from the system in accordance with applicable taws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.
SI-12	Information Management and Retention	C-SCRM should be included in information management and retention requirements, especially when the sensitive and proprietary information of a system integrator, supplier, or external service provider is concerned.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (i) Retain Personal Data (PD), including metadata, for an organization- defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and	5	Manage and retain information within the system and information output from the system in accordance with applicable taws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.
SI-20	Tainting	Suppliers, developers, system integrators, external system service providers, and other ICI/OT-related service providers may have access to the sensitive information of a federal agency, in this instance, enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.	Functional	Equal	Tainting	THR-08	Mechanisms exist to embed false data or steganographic data in files to enable the organization to determine if data has been exfiltrated and provide a means to identify the individual(s) involved.	10	Embed data or capabilities in the following systems or system components to determine if organizational data has been edifitrated or improperly removed from the organization: (Assignment: organization-defined systems or system components).
SR-1	Policy and Procedures	CSCRM policies are developed at Level 1 for the overall enterprise and at Level 2 for specific missions and functions. C-SCRM policies can be implemented at Levels 1, 2, and 3, depending on the level of depth and function. C-SCRM pockedures are developed at Level 2 for specific missions and functions and at Level 3 for specific posterns. Enterprise functions including but not limited to information security, legal, risk management, and acquisition should review and concur on the development of C-SCRM policies and procedures or provide guidance to system owners for developing system-specific C-SCRM procedures.	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	Develop, document, and disseminate to [Assignment. organization-defined personnel or roles]:     [Selection (one or more): Organization-level; Mission/Dusiness process-level; System-level] supply chain risk management policy that: (all Addresses purpose, soope, roles.)
SR-1	Policy and Procedures	CSCRM policies are developed at Level 1 for the overall enterprise and at Level 2 for specific missions and functions. C-SCRM policies can be implemented at Levels 1, 2, and 3, depending on the level of depth and functions. C-SCRM pocifications and at Level 3 for specific missions and functions and at Level 3 for specific posterns. Enterprise functions including but not limited to information security, legal, risk management, and acquisition should review and concur or the development of C-SCRM policies and procedures or provide guidance to system owners for developing system-specific C-SCRM procedures.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	Develop, document, and disseminate to [Assignment. organization-defined personnel or roles]:     (Selection (one or more): Organization-level; Mission/Dusliness process-level; System-level] supply chain risk management policy that: (a) Addresses purpose. scooe. roles.
SR-1	Policy and Procedures	CSCRM policies are developed at Level 1 for the overall enterprise and at Level 2 for specific missions and functions. CSCRM procedures are developed at Level 2 for specific missions and functions and state of the specific missions and functions and at Level 3 for detail. C-SCRM procedures are developed at Level 2 for specific missions and functions and at Level 3 for specific systems. Enterprise functions including but not intrinsic to information security, legal, risk management, and acquisition should review and concur on the development of C-SCRM pioceles and procedures or provide guidance to system owners for developing systems-specific CSCRM procedures.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:     [Selection (one or more): Organization-level; Mission/Dusiness process-level; System-level] supply chain risk management policy that:     [al Addresses purpose, scoep. roles.
SR-2	Supply Chain Risk Management Plan	C-SCRM plans describe implementations, requirements, constraints, and implications at the system level. C- SCRM plans are influenced by the enterprise's other risk seasonem activities and may inherial and allori common control baselines defined at Level 1 and Level 2. C-SCRM plans defined at Level 3 work in collaboration with the enterprise's C-SCRM Strategy and Potioles (Level 1 and Level; 2) and the C-SCRM implementation Plan, Level 1 and Level; 2 to provide a systematic and holistic approach for cybersecurify supply chain risk management across the enterprise.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plant for Supply Chain Risk Management (SCPM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: (Assignment: organization-defined
SR-2	Supply Chain Risk Management Plan	CSCRM plans describe implementations, requirements, constraints, and implications at the system level. C- SCRM plans are influenced by the enterprise's other risk assessment activities and may inherit and tailor common control baselines defined at Level 1 and Level 2.—SCRM plans defined at Level 3 work in collaboration with the enterprise's C-SCRM Strategy and Policies (Level 1 and Level; 2) and the C-SCRM Implementation Plan (Level 1 and Level) 2 porvide's a systematic and holistic approach for cybersecurity supply chain risk management across the enterprise.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to:  (1) Evaluate security risks and threats associated with Technology Assets, Applications and Ard's Services (TAKS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: Sasjamment: organization-defined
SR-3	Supply Chain Controls and Processes	Section 2 and Appendix C of this document provide detailed guidance on implementing this control. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity.	Functional	Equal	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	10	a. Establish a process or processe to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnels.
SR-3(1)	Supply Chain Controls and Processes   Diverse Supply Base	Enterprises should diversify their supply base, especially for critical ICT/OT products and services. As a part of this exercise, the enterprise should attempt to identify single points of failure and risk among primes and lower-level entitles in the supply chain. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis.	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Nechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flaved and/or malformed software.	5	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].
SR-3(1)	Supply Chain Controls and Processes   Diverse Supply Base	Enterprises should diversify their supply base, especially for critical ICT/OT products and services. As a part of this exercise, the enterprise should attempt to identify single points of failure and risk among primes and lower-level entities in the supply chain. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis.	Functional	Intersects With	Supplier Diversity	TDA-03.1	Mechanisms exist to obtain cybersecurity and data protection technologies from different suppliers to minimize supply chain risk.	5	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].
SR-3(1)	Supply Chain Controls and Processes   Diverse Supply Base	Enterprises should diversify their supply base, especially for critical ICT/OT products and services. As a part of this exercise, the enterprise should attempt to identify single points of failure and risk among primes and lower-level entitles in the supply chain. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis.	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tallored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	5	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].



Secure Controls Framework (SCF) 22 of 23

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM	STRM	SCF Control	SCF#	Secure Controls Framework (SCF)	Strength of Relationship	Notes (optional)
		NIST SP 800-161 R1 Supplemental C-SCRM Guidance  Enterprises should require their prime contractors to implement this control and flow down this requirement	Hationale	Kelationship			Control Description  Mechanisms exist to require contractual requirements for cybersecurity	/ontionall	. , ,
SR-3(3)	Supply Chain Controls and Processes   Sub-tier Flow Down	to relevant sub-tier contractors throughout the SDLC. The use of the acquisition process provides an important which is optimed the subject with a part of procurement requirements, interprises should include the need for suppliers to flow down controls to subcontractors throughout the SDLC. As part of market research and analysis activities, enterprises should conduct houst due diligence research on professional suppliers or products, as well as their upstream dependencies (e.g., fourth- and fifth-party suppliers), which can be on retoring a world inside point of failure within their supplier supplier suppliers and indicate the suppliers and indicate the suppliers of failure within their suppliers in suppliers a result of this research.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.
SR-3(3)	Supply Chain Controls and Processes   Sub-tier Flow Down	Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-life contractors throughout the SQLC. The use of the acquisition process provides an important vehicle to protect the supply chain. As part of procurement requirements, enterprises should include the need for suppliers to flow down controls to subcontractors throughout the SDLC. As part of market research and analysis activities, enterprises should conduct robust due diligence research on potential suppliers or products, as well as their upsteam dependencies (e.g., louth- and fifth-party suppliers), which can be an enterprise and single product of failure within their supply chains. The results of this research can	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.
SR-4	Provenance	Provenance should be documented for systems, system components, and associated data throughout the SDLC. Enterprises should consider producing SDMPs for pagicable and appropriate classes of software, including purchased software, open source software, and in-house software. SBDMs should be produced using only NTLA-supported SBDM formats that can satisfy INTLA SBDM job 14028 NTLA minimum SBDM elements. Enterprises producing SBDMs should use [NTLA SBDM] for 14028 NTLA minimum SBDM elements as thaming for the inclusion of primary components. SBDMs should be digitally signed using a verifiable and trusted key. SBDMs can date a critical trelia mebiliary contribution to constitution of SBDMs can date a critical trelia mebiliary contributions.	Functional	Intersects With	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to systems, system components and associated data.	5	Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: [Assignment: organization-defined systems, system components, and associated data].
SR-5	Acquisition Strategies, Tools, and Methods	Section 3 and SA controls provide additional guidance on acquisition strategies, tools, and methods. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity.	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize failored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	5	Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods].
SR-6	Supplier Assessments and Reviews	In general, an enterprise should consider any information pertinent to the security, integrify, restlence, quality, trustworthines, or authenticity of the supplier of their provided services or products. Enterprises should consider applying this information against a consistent set of cone baseline factors and assessment criteria to facilitate equitable comparison (between suppliers and over time). Depending on the specific context and purpose for which the assessment is being conducting, the enterprise may select additional factors. The quality of information (e.g., its relevance, completeness, accuracy, etc.) relief upon for an assessment is also an immortant consideration. Reference accuracy for assessment information should also	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	5	Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [Assignment: organization-defined frequency].
SR-7	Supply Chain Operations Security	The C-SCRM PMO can help determine OPSEC controls that apply to specific missions and functions. OPSEC controls are particularly important when there is specific concern about an adversarial threat from or to the mission or business operations, its information, and/or its service/product offerings make it a more attractive target for an adversarial threat.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	Employ the following Operations Security (OPSEC) controls to protect supply chain-related information for the system, system component, or system service: [Assignment: organization-defined Operations Security (OPSEC) controls].
SR-7	Supply Chain Operations Security	The C-SCRM PMO can help determine OPSEC controls that apply to specific missions and functions. OPSEC controls are particularly important when there is specific concern about an adversariat threat from or to the enterprise's supply chain or an element within the supply chain, or when the nature of the enterprise's mission or business operations, its information, and/or its service/product offerings make it a more attractive target for an adversarial threat.	Functional	Intersects With	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	5	Employ the following Operations Security (OPSEC) controls to protect supply chain-related information for the system. system component, or system service: [Assignment or granization-defined Operations Security (OPSEC) controls].
SR-8	Notification Agreements	At minimum, enterprises should require their suppliers to establish notification agreements with entities within their supply chain that have a role or responsibility related to that critical service or product. Departments and agencies should refer to Appendix F to implement this guidance in accordance with Executive Order 14029, improving the Nation's Cybersecurity.	Functional	Equal	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technicogy Assets, Applications and/or Services (TAAS) that the organization utilizes.	10	Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [Selection (one or more): notification of supply chain compromises; results of assessments or audits; [Assignment: organization-defined information].
SR-9	Tamper Resistance and Detection	Enterprises should apply tamper resistance and detection control to critical components, at a minimum. Criticality analysis can help determine which components are critical. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis. The C-SCRM PMO can help identify critical components, especially those that are used by multiple missions, functions, and systems within an enterprise. Departments and agencies should refer to Appendix FD implement this guidance in accordance with Executive Order 1000, Improving the Nation's Cybersecurity.	Functional	Intersects With	Logical Tampering Protection	AST-15	Mechanisms exist to verify logical configuration settings and the physical integrity of critical technology assets throughout their lifecycle.	5	Implement a tamper protection program for the system, system component, or system service.
SR-10	Inspection of Systems or Components	Enterprises should inspect critical systems and components, at a minimum, for assurance that tamper resistance controls are in place and to examine whether there is evidence of tampering. Products or components should be inspected prior to use and periodically threather. Inspection requirements should also be included in contracts with suppliers, developers, system integrators, external system service providers, and other ICDOT-related experie providers. Enterprise should require their prime contractors to implement this control and flow down this requirement to relevant sub-sier contractors and flow down to subcontractors, when relevant.	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampening and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5	Inspect the following systems or system components [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection] to detect tampering: [Assignment: organization-defined systems or system components].
SR-10	Inspection of Systems or Components	Enterprises should inspect critical systems and components, at a minimum, for assurance that tamper resistance controls are in place and to examine whether there is evidence of tampering. Products or components should be inspected prior to use and periodic sally thereafter. Inspection requirements should also be included in contracts with suppliers, developers, system integrators, external system service providers, and other ICTOT-related exerce providers. Amonther the priories contractors to implement this control and flow down this requirement to relevant sub-sier contractors and flow down to subcontractors, when relevant.	Functional	Intersects With	Technology Asset Inspections	AST-15.1	Mechanisms exist to physically and logically inspect critical technology assets to detect evidence of tampering.	5	Inspect the following systems or system components [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering; [Assignment organization-defined systems or system components].
SR-11		The development of and counterfest policies and pnoedures requires input from and coordination with acquisition, information technology, IT security, legal, and the C-SCRM PMO. The policy and procedures should address registary compliance requirements, contract requirements or clauses, and counterfest reporting processes to enterpresses, such as GIGEP and/or other appropriate enterprises. Where applicable and appropriate, the policy should also address the development and use of a qualified bidders list (QRL) and/or qualified manufactures list (QRL). This helps prevent counterfest through the use of authorized suculess, wherever possible, and their interaction in the organization's supply-kin (CSR SCRM WG3).	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampening and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5	So Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and b. Report counterfeit components to ISBelection (one or more): source of counterfeit components to ISBelection (one or more): source of counterfeit and the system; and the system components to ISBelection (one or more): source of counterfeit component; IASSIGNENT, or accompanied to the system component is source of counterfeit or more controlled to the system counterfeit or system component is source of counterfeit or more controlled to the system counterfeit or component is system component in the system counterfeit or component is system counterfeit or component in the system counterfeit or component is system to the system counterfeit or controlled to the system counterfeit or controlled to the system counterfeit or counterfeit or controlled to the system component is system to the system component in the system component is controlled to the system component in the system component is controlled to the system component in the system component is controlled to the system component in the system component is controlled to the system component in the system component is controlled to the system component in the system component is controlled to the system component in the system component is controlled to the system component in the system component is controlled to the system component in the system controlled to the system component in the system component in the system controlled to
SR-11(1)	Component Authenticity   Anti-counterfeit Training	The C-SCRM PMO can assist in identifying resources that can provide anti-counterfeit training and/or may be shall to conduct such training for the enterprise. The C-SCRM DMO can also sesist in identifying which.	Functional	Equal	Anti-Counterfeit Training	TDA-11.1	Mechanisms exist to train personnel to detect counterfeit system components, including hardware, software and firmware.	10	Train [Assignment: organization-defined personnel or roles] to detect counterfeit system components (including hardware, software, and firmware).
SR-11(2)	Component Authenticity   Configuration Control for Component Service and Repair	Information technology, IT security, or the C-SCRM PMO should be responsible for establishing and implementing configuration control processes for component service and repair, to include – If applicable – integrating component service and repair into the overall enterprise configuration control processes. Component authenticity should be addressed in contracts when procuring component servicing and repair support.	Functional	Equal	Maintain Configuration Control During Maintenance	MNT-07	Mechanisms exist to maintain proper physical security and configuration control over technology assets awaiting service or repair.	10	Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service (Assignment: organization- defined system components).
SR-11(3)	Component Authenticity   Anti-counterfeit   Scanning	Enterprises should conduct anti-counterfeit scanning for critical components, at a minimum. Criticality analysis can help determine which components are critical and should be subjected to this scanning. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis. The C-SCRM PMO can help dentify critical components, especially those used by multiple missions, functions, and systems within an enterprise.	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampening and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5	Scan for counterfeit system components [Assignment: organization-defined frequency].
SR-12	Component Disposal	If security – in coordination with the C-SCRM PMO – can help establish appropriate component disposal policies, procedures, mechanisms, and techniques.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	Dispose of [Assignment: organization-defined data, documentation, tools, or system components] using the following techniques and methods: (Assignment: organization-defined techniques and methods):
SR-12	Component Disposal	If security – in coordination with the C-SCRM PMO – can help establish appropriate component disposal policies, procedures, mechanisms, and techniques.	Functional	Intersects With	Component Disposal	TDA-11.2	[deprecated - incorporated into AST-09] Mechanisms exist to dispose of system components using organization- defined techniques and methods to prevent such components from entering the gray market.	5	Dispose of [Assignment: organization-defined data, documentation, tools, or system components] using the following techniques and methods: [Assignment: organization-defined techniques and methods].
SR-13	Supplier Inventory	a Develop, document, and maintain an inventory of suppliers that:  Accurately and minimally reflects the organization's liter one suppliers that may present a cybersecurity risk in the supply chain [Assignment organization-defined parameters for determining liter one supply chain; 2. Is at the level of granularity deemed necessary for assessing criticality and supply chain risk, tracking, and reporting.  3. Documents the following information for each tier one supplier (e.g., prime contractor): review and update supplier into the supplier of the properties.	Functional	Subset Of	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentially, integrity, Availability and/or Sately (CSA) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	10	This specific NIST 800-161 R1 control does not exist in NIST 800-53 R5.

