

Cybersecurity and Supply Chain Risk Management and BEAD

April 2023



Table of Contents

3	Why are Cybersecurity and SCRM Important to BEAD?
5	What are the NOFO Requirements for Cybersecurity?
7	What is the NIST Cybersecurity Framework?
12	What is Executive Order 14028?
15	How do I Develop a Cybersecurity Plan with Those Resources?
17	What are the NOFO Requirements for SCRM?
21	What is the NIST Publication NISTIR 8276?
25	What is NIST 800-161?
29	How do I Develop a SCRM Plan with Those Resources?
31	What are Eligible Uses of Program Funds for Cyber Skills?
34	NTIA's Communications Supply Chain Risk Information Partnership (C SCRIP)
37	What are the Next Steps?



Why are Cybersecurity and SCRM Important to BEAD?

Why are they Important to BEAD?

ISPs interested in deploying BEAD-funded broadband networks must have strong cybersecurity and SCRM plans.

ISP Subgrantee Responsibility

ISP subgrantees that receive BEAD broadband deployment subgrants will be responsible for maintaining cyber and SCRM plans. We'll spend most of today discussing what the BEAD NOFO requires of those plans and resources available to help ISPs meet the requirements.

State and Territory Responsibility

States and territories must provide a way for prospective subgrantees to attest to having adequate cybersecurity and SCRM plans in place.



What are the NOFO Requirements for Cybersecurity?

BEAD NOFO Cybersecurity Requirements

Prior to allocating any funds to a subgrantee, an Eligible Entity must require a prospective subgrantee to attest to 4 requirements relating to cybersecurity.



BEAD NOFO Section IV.C.2.c.vi Program Structure, Sequencing and Requirements; Program Requirements; Obligations for Subgrantees Deploying Network Projects; Service Obligations; Cybersecurity and Supply Chain Risk Management



The prospective subgrantee has a **cybersecurity risk management plan** (the plan) **in place** that is either:

- a. **operational**, if the prospective subgrantee is providing service prior to the award of the grant; or
- b. **ready to be operationalized upon providing service**, if the prospective subgrantee is not yet providing service prior to the grant award;



The plan reflects the latest version of the **National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity** (currently Version 1.1) and the **standards and controls set forth in Executive Order 14028** and specifies the security and privacy controls being implemented;



The plan will be **reevaluated and updated on a periodic basis** and as events warrant; and



The **plan will be submitted to the Eligible Entity prior to the allocation of funds. If the subgrantee makes any substantive changes** to the plan, **a new version will be submitted to the Eligible Entity within 30 days**. The Eligible Entity must provide a subgrantee's plan to NTIA upon NTIA's request.



What is the NIST Cybersecurity Framework (CSF)?

Cybersecurity Framework Attributes

The NIST Cybersecurity Framework helps organizations reduce their cybersecurity risks and is widely recognized as foundational to securing organizations & technology.

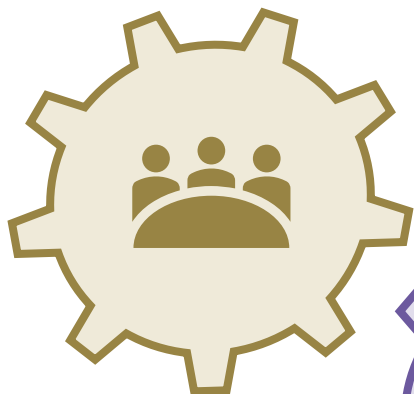
ATTRIBUTES

- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Risk-based
- Based on international standards
- Guided by many perspectives – private sector, academia, public sector
- Align legal/regulatory requirements and organizational and risk management priorities



Cybersecurity Framework

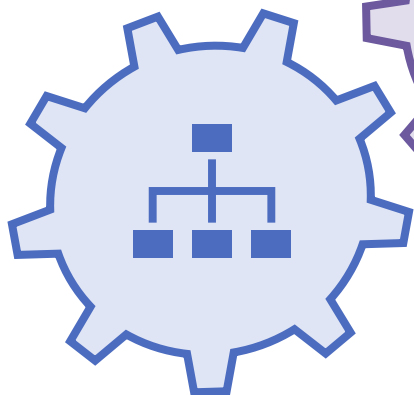
There are three main aspects to the NIST Cybersecurity Framework: the Core, Profiles, and Implementation Tiers.



The **Core** provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy or cybersecurity risk, based on international standards



Profiles are a selection of specific Functions, Categories, and Subcategories from the Core that the organization has prioritized to help it manage cybersecurity risk



Implementation Tiers help an organization communicate about whether it has sufficient processes and resources in place to manage cybersecurity risk and achieve its Target Profile

Cybersecurity Framework Core

There are many functions and categories when it comes to the Cybersecurity Framework Core.

Function (5)	Category (23)	Subcategories (108)	Informative References
Identify (ID)	Asset Management		
	Business Environment		
	Governance		
	Risk Assessment		
	Risk Management Strategy		
Protect (PR)	Supply Chain Risk Management		
	Identity Management & Access Control		
	Awareness and Training		
	Data Security		
	Information Protection Procedures		
Detect (DE)	Maintenance		
	Protective Technology		
	Anomalies and Events		
Respond (RS)	Security Continuous Monitoring		
	Detection Processes		
	Response Planning		
Recover (RC)	Communications		
	Analysis		
	Mitigation		
	Improvements		
	Recovery Planning		
	Improvements		
	Communications		

Function	Category	Subcategory	Informative References
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	CIS CSC, 16 COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 ISO/IEC 27001:2013, A.7.1.1, A.9.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	CIS CSC 1, 12, 15, 16 COBIT 5 DSS05.04, DSS05.10, DSS06.10 ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

Journey to Cybersecurity Framework 2.0

NIST continually updates the CSF to keep it up-to-date and accurate.



NIST has begun the process of updating the Cybersecurity Framework.



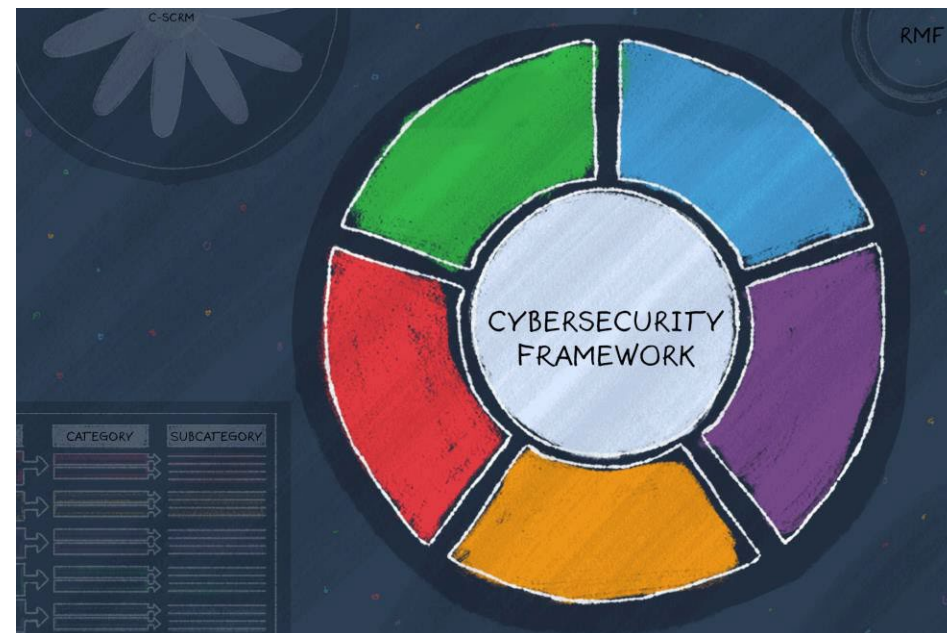
The update will address the evolving cybersecurity risk and standards landscape and make it easier for organizations to address risks.



NIST is actively relying on and seeking diverse stakeholder feedback in the update process.



Ways to engage: <https://www.nist.gov/cyberframework>





What is Executive Order 14028?

What is Executive Order 14028?

Executive Order 14028: Improving the Nation's Cybersecurity was signed by President Biden on May 12, 2021.



The Executive Order lays out several initiatives designed to **modernize cybersecurity defenses** by protecting Federal networks, improving information-sharing between the U.S. government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur.



This Executive Order is in **response to the SolarWinds, Microsoft Exchange, and Colonial Pipeline incidents**, which took place in late 2020 and early 2021.



While Executive Orders pertain to the executive branch of the Federal government, Executive Order 14028 has **several requirements that apply to private sector IT and OT service providers** when these companies enter into a contract to conduct an array of day-to-day functions on Federal Information Systems.



For example, a private sector service provider for a Federal agency **must report when they discover a cyber incident** involving a software product or service provided to that agency.



More information about these requirements can be found in the **Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS)**.

How Does Executive Order 14028 Apply to BEAD?

The Executive Order has direct implications for ISPs receiving BEAD broadband deployment subgrants.



BEAD NOFO Section IV.C.2.c.vi Program Structure, Sequencing and Requirements; Program Requirements; Obligations for Subgrantees Deploying Network Projects; Service Obligations; Cybersecurity and Supply Chain Risk Management:

The plan reflects the latest version of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (currently Version 1.1) and ***the standards and controls set forth in Executive Order 14028*** and specifies the security and privacy controls being implemented;



The requirements laid out in Executive Order 14028 **apply to private sector companies who contract with the Federal government** to provide IT and OT services.



While BEAD is a Federal grant program, **subgrantees who receive funds are not automatically considered to be contracting with the Federal government.**



In cases which the Federal government procures services provisioned over the BEAD-funded network, the network must satisfy the **special requirements set out in the FAR and the DFARS** pursuant to the EO.



The prospective BEAD subgrantee's cybersecurity plan should "reflect" the fact that, if the provider seeks to contract with the Federal government, it will be **prepared to satisfy the pertinent requirements.**



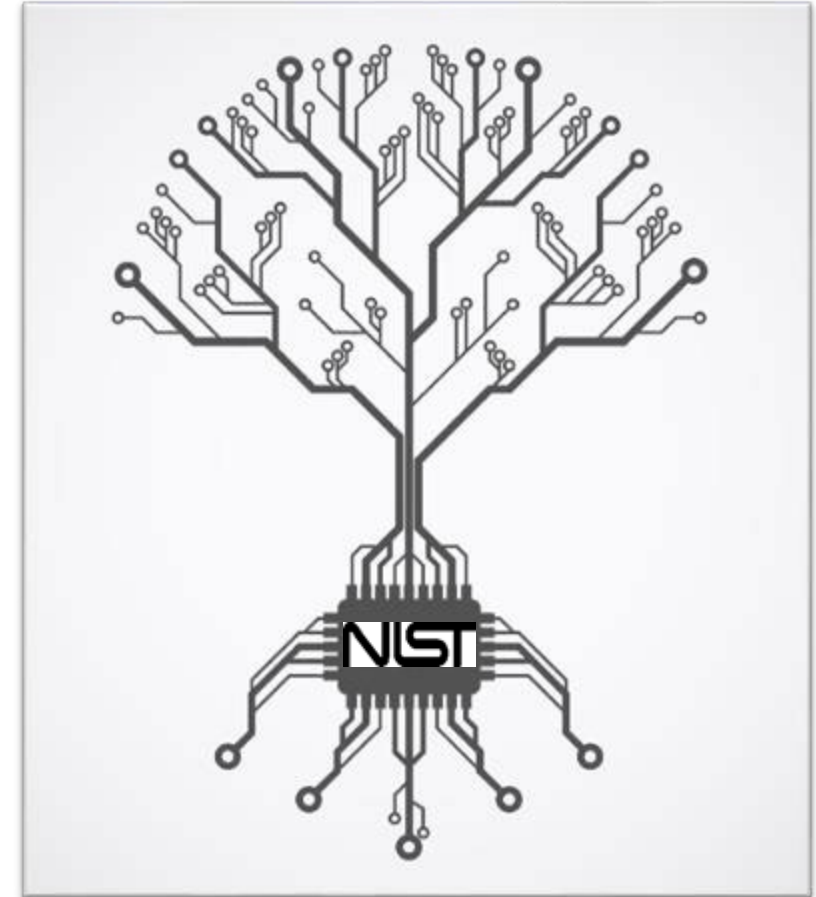
How Do I Develop a Cybersecurity Risk Management Plan?

Sample Profiles and Guidance

NIST provides the following sample profiles and guidance to assist with cybersecurity risk management.

RESOURCES

- **CSF Resources:**
 - [Risk Management Resources](#)
 - [Quick Start Guide](#)
- **Communications-Specific Resources:**
 - Federal Communications Commission (FCC) Communications, Security, Reliability and Interoperability Council's (CSRIC) [Cybersecurity Risk Management and Best Practices Working Group 4: Final Report](#) (contains CSF profiles for broadcast, satellite, cable, wireline, and wireless)
 - NTCA–The Rural Broadband Association's [Sector-Specific Guide for Small Network Service Providers](#)
- **Small Business Resources:**
 - [Small Business Cybersecurity Corner](#) provides actionable resources to help small businesses identify, assess, manage, and reduce their cybersecurity risks.





What are the NOFO Requirements for Supply Chain Risk Management (SCRM)?

BEAD NOFO Cybersecurity Requirements

Prior to allocating any funds to a subgrantee, an Eligible Entity must require a prospective subgrantee to attest to 4 requirements relating to cybersecurity.



BEAD NOFO Section IV.C.2.c.vi Program Structure, Sequencing and Requirements; Program Requirements; Obligations for Subgrantees Deploying Network Projects; Service Obligations; Cybersecurity and Supply Chain Risk Management



The prospective subgrantee has a SCRM plan in place that is either:

- a. **operational**, if the prospective subgrantee is already providing service at the time of the grant; or
- b. **ready to be operationalized upon providing service**, if the prospective subgrantee is not yet providing service prior to the grant award;



The plan is based upon the **key practices discussed** in the **NIST publication NISTIR 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*** and related SCRM guidance from NIST, including **NIST 800-161, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*** and specifies the supply chain risk management controls being implemented;



The plan will be **reevaluated and updated on a periodic basis** and as events warrant; and



The **plan will be submitted to the Eligible Entity prior to the allocation of funds. If the subgrantee makes any substantive changes** to the plan, **a new version will be submitted to the Eligible Entity within 30 days**. The Eligible Entity must provide a subgrantee's plan to NTIA upon NTIA's request.

Cybersecurity Supply Chain Risk Management

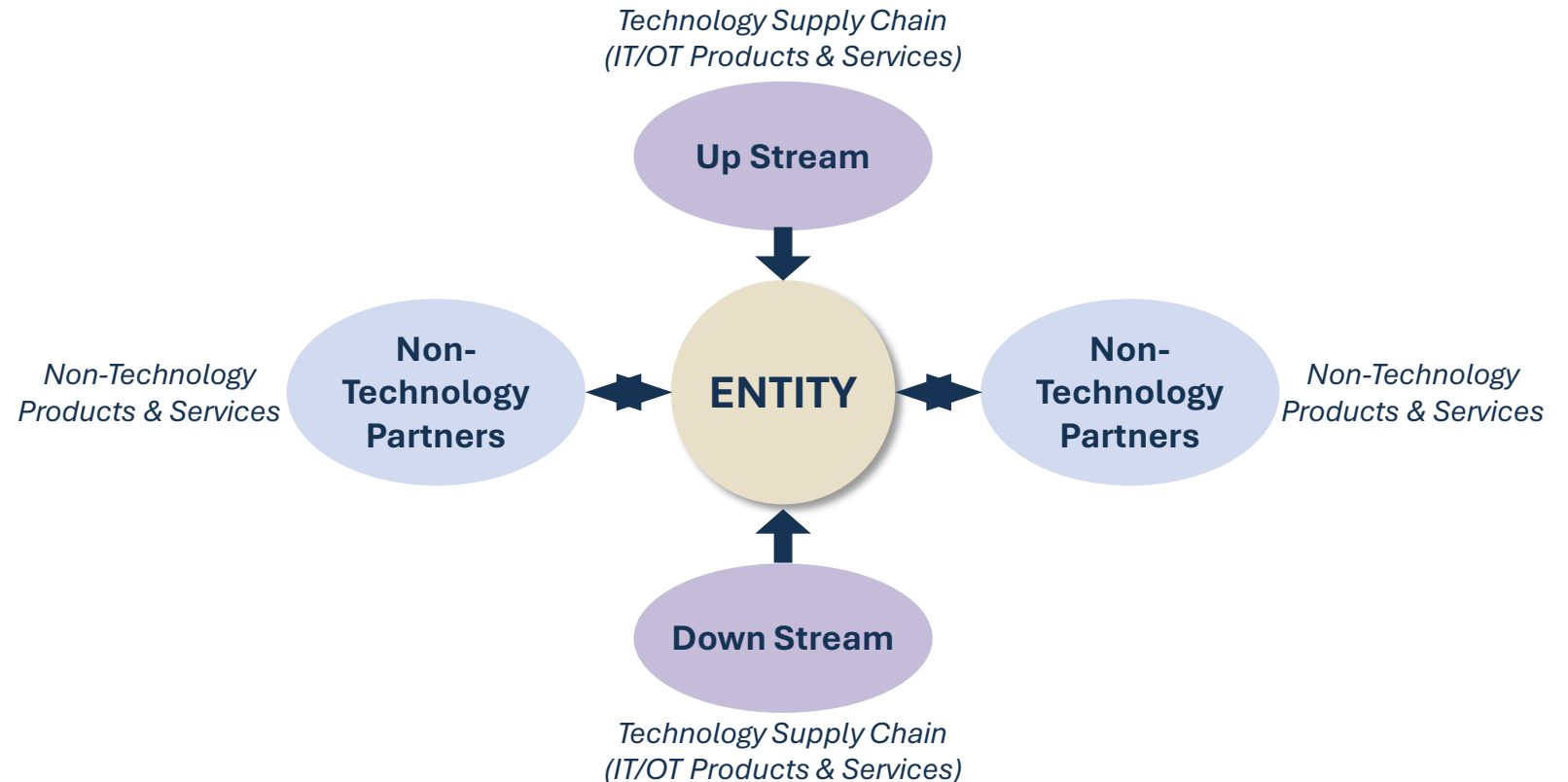
Cybersecurity risk in supply chains refers to the potential for harm or compromise that may arise from suppliers, their supply chains, their products, or their services. Cybersecurity risk in supply chains is the result of threats that exploit vulnerabilities or exposures within 1) products and services that traverse supply chains; or 2) supply chains themselves.

TRUST

- Organization
- Process
- Products/Service

BUT VERIFY

- Due Diligence
- Standards/Conformity Assessments
- Testing/Audits



Cybersecurity Threats and Vulnerabilities in Supply Chains (Examples)

Examples of cybersecurity threats and vulnerabilities in supply chains:



Counterfeit products



Hardware or software delivered with malware or malware inserted post-delivery



Hardware/software with unwanted functionality



Third and Nth Party – Vulnerabilities in systems and networks used by supply chain partners



Insider Threat (including non-adversarial)



Poor quality manufacturing, development, maintenance, or disposal practices



Supply chain disruptions



Theft/alteration of system data



What is NIST Publication NISTIR 8276?

NISTIR 8276: Key Practices in C-SCRM

There are 8 key practices when using NISTIR 8276.



24 Recommendations—References Mapping (I/II)

	NIST SP 800-161	NISTIR 7622	2015 Case Studies	2019 Case Studies	CSF	FSP	UTC	ISO/IEC 27002	ISO/IEC 27036	ISO/IEC 20243
Establish supply chain risk councils to include executives from across the organization (cyber, product security, procurement, ERM, business units, etc.)	✓		✓	✓	✓	✓				
Create explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, and physical security functions			✓	✓		✓				✓
Increase board involvement in C-SCRM through regular risk discussions and sharing of measures of performance			✓	✓		✓				
Integrate cybersecurity considerations into system and product lifecycle	✓	✓	✓	✓	✓	✓		✓	✓	✓
Clearly define roles and responsibilities for security aspects of specific supplier relationships	✓		✓	✓		✓	✓	✓	✓	✓
Use master requirements list and SLAs to establish requirements with suppliers	✓		✓	✓			✓	✓	✓	✓
Propagate security requirements to supplier's sub-suppliers	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Train key stakeholders in your organization and within supplier organization	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Terminate supplier relationships with security in mind	✓	✓		✓		✓	✓	✓	✓	✓
Use Criticality Analysis Process Model or BIA to determine supplier criticality	✓			✓			✓	✓	✓	
Establish visibility into your suppliers production processes to capture, e.g., defect rates, causes of failure, and testing		✓	✓	✓					✓	✓
Know if your data and infrastructure are accessible to supplier's sub-suppliers	✓			✓				✓	✓	✓
Mentor and coach suppliers to improve their cybersecurity practices	✓		✓	✓	✓	✓	✓			✓

24 Recommendations—References Mapping (II/II)

	NIST SP 800-161	NISTIR 7622	2015 Case Studies	2019 Case Studies	CSF	FSP	UTC	ISO/IEC 27002	ISO/IEC 27036	ISO/IEC 20243
Require use of the same standards within acquirer and supplier organizations				✓						
Use acquirer assessment questionnaires to influence acquirer cybersecurity requirements				✓						
Include key suppliers in IR, DR, and CP plans and tests	✓		✓	✓	✓	✓	✓	✓	✓	
Maintain a watchlist of "Issue Suppliers" for the suppliers who had issues in the past and acquirer should be cautious about the future use. Supplier should be used only after approval from council				✓						
Establish remediation acceptance criteria for the identified risks	✓			✓		✓		✓	✓	
Establish cybersecurity requirements through Security Exhibit / Security Schedule / Security Addendum document. This document should be finalized in partnership with the risk council members and included in all Master Services Agreements (MSAs) of all suppliers based on the risk associated with the supplier engagement				✓						
Establish protocols for vulnerability disclosure and incident notification	✓		✓	✓	✓	✓	✓	✓	✓	✓
Establish protocols for communications with external stakeholders during incidents	✓		✓	✓	✓	✓	✓	✓	✓	
Collaborate on lessons learned and update joint plans based on lessons learned	✓		✓	✓	✓	✓	✓	✓	✓	✓
Use third party assessments, site visits, and formal certification to assess critical suppliers	✓		✓	✓	✓	✓	✓	✓	✓	✓
Have plans in place for supplied product obsolescence	✓	✓					✓	✓	✓	✓



What is NIST 800-161? Rev.1

SP 800-161 Rev.1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

SP 800-161 Rev.1 provides guidance and tips for those creating supply chain risk management plans.

"Audience profiles and user guide"	Integrates C-SCRM into broader ERM activities & Across Layers of Organization	Guidance on development of a C-SCRM Program Management function	Adds Foundational, Sustaining, and Enhancing Key Practices
Modular Organization <ul style="list-style-type: none">• Main Body• Multiple Appendices	Critical Success Factors: <ul style="list-style-type: none">• C-SCRM in Acquisition• SC Information Sharing• Training & Awareness• Key Practices• Measures and Measurement	Appendix E on FASCSA and Appendix F on EO 14028 Section 4(d), Software Supply Chain Security	Adds Foundational, Sustaining, and Enhancing Key Practices

SP 800-161 Appendices

SP 800-161 provides the following appendices for additional guidance and context.



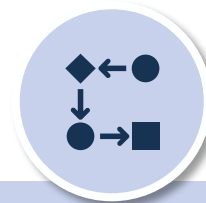
C-SCRM Controls

- Baseline Controls
- RMF Level
- “Flow-down” Controls



Risk Exposure Framework

- Sample Risk Exposure Framework
- Threat Scenarios Examples



C-SCRM Activities in the Risk Management Process

- Describes Tasks for Each C-SCRM Process



Templates

- Strategy & Implementation Plan
- Policy
- C-SCRM (System-level) Plan
- C-SCRM Risk Assessment

800-161 Appendix F: Guidance for Software Supply Chain Security

NIST implementation of EO 14028 Sections 4(c)/(d):

Software supply chain security concepts are a critical sub-discipline within C-SCRM

Available online to allow for update to guidance.



<https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains>

EO through the lens of 800-161

EO Critical Software & Measures

Software Verification

SSDF & Attestations

Emerging Concepts

Software Bill of Materials (SBOM)

Enhanced Vendor Risk Assessments

Open Source Software Controls

Vulnerability Management










How Do I Develop a Supply Chain Risk Management Plan?

How Do I Develop an SCRM Plan?

An SCRM Plan must be a Strategy and Implementation Plan (per SP 800-161r1, Appendix D)

The purpose of a strategy and implementation plan is to provide a strategic roadmap for implementing effective C-SCRM capabilities, practices, processes, and tools within the enterprise in support of its vision, mission, and values. The C-SCRM strategy and implementation plan should anchor to the overarching enterprise risk management strategy and comply with applicable laws, executive orders, directives, and regulations.

Sample components to a strategy and implementation plan:

-  Authorities and Compliance (external factors, such as laws, regulations, customer requirements, etc.)
-  Strategic Objectives
-  Implementation Plan and Progress Tracking
-  Internal policies (those in place, those that need developed, and those that need revised...template also in Appendix D)
-  Roles and Responsibilities
-  Definitions
-  Revision and Maintenance (iterative process)



What are Eligible Uses of Program Funds for Cyber Skills?

What are Eligible Uses of BEAD Funds for Cyber?

The BEAD Program allow the use of funds for cyber-related activities.


BEAD:

Eligible uses of funding in connection with last-mile broadband deployment projects include:

- Network software upgrades, including, but not limited to, cybersecurity solutions
- Training for cybersecurity professionals who will be working on BEAD-funded networks

Eligible non-deployment uses include:

- User training with respect to cybersecurity, privacy, and other digital safety matters
- Computer science, coding and cybersecurity education programs



NTIA's Communications Supply Chain Risk Information Partnership (C-SCRIP)

C-SCRIP

The Communications Supply Chain Risk Information Partnership (C-SCRIP) is an information sharing program that shares supply chain security risk information with trusted communications providers and suppliers.



Our goal is to improve small and rural communications providers' and equipment suppliers' access to information about risks to key elements in their supply chain.



The C-SCRIP program is complementary to the FCC "rip and replace" program to reimburse smaller providers for removing and replacing insecure equipment and services in U.S. networks.



In addition to supply chain risk information, C-SCRIP shares cybersecurity alerts, guidance on ransomware incidents, and relevant training events with this community.



As we were planning the program, we heard from private-sector stakeholders that unclassified information will be the most useful for organizations to receive.

C-SCRIP

C-SCRIP publishes a bi-monthly newsletter with the latest information from NTIA and other Federal partners. You can also access these resources through the C-SCRIP website, **cscrip.ntia.gov**.





What are the Next Steps?

What are the Next Steps?

- ✓ **States must require attestations that plans are or will be in place**
 - ISPs must submit plans to states prior to funds allocation
 - Subsequent changes to plans must be submitted within 30 days
 - States may propose additional measures to safeguard networks and users

- ✓ ISPs interested in subgrants must **develop or update cybersecurity and SCRM plans** and obtain attestations if relying on third party networks

- ✓ We'll offer **insight as Framework 2.0 is released** for comment and eventually published

Thank you!

