Tribal Broadband Connectivity Program: Cybersecurity and Supply Chain Risk Management

February 15, 2024

Housekeeping

Questions

- Type questions in the Q&A box on the right-hand side of the screen. Questions and answers will be available on the FAQ section of our website
- Notice of Funding Opportunity

Presentation

- The presentation along with a transcript and recording will be available on the BroadbandUSA website under Round Two Notice of Funding Opportunity of the Tribal Broadband connectivity Funding Program

This presentation is for informational purposes only and is intended solely to assist applicants in better understanding the NTIA Tribal Broadband Connectivity Program, and the requirements set forth in the program's second Notice of Funding Opportunity (Second TBCP NOFO). This presentation does not and is not intended to supersede, modify, or otherwise alter applicable statutory or regulatory requirements, or the specific application requirements set forth in the Second TBCP NOFO. In all cases, statutory and regulatory mandates and the requirements set forth in the Second TBCP NOFO shall prevail over any inconsistencies contained in this presentation.

Presenters

Presenters:

- Crystal Hottowe, Federal Program Officer

Moderator:

- Isabel Lopez, Federal Program Officer, Team Lead

Panelists:

- Jeff Kozdron, Federal Program Officer
- Gabe Montoya, Federal Program Officer

Agenda

1. Why are Cybersecurity and SCRM Important to TBCP?
2. What are the NOFO 2 Requirements for Cybersecurity?
3. How do I Develop a Cybersecurity Risks Mitigation Plan?
4. What are the NOFO 2 Requirements for SCRM?
5. What is Supply Chain Risk Management & How do I Develop an SCRM Plan?

Why are Cybersecurity and SCRM Important to TBCP?

Why are Cybersecurity and SCRM Important to TBCP?

NTIA recognizes the importance of protecting American communications networks and those who use them from domestic and international threat actors. TBCP is meant to promote the natural evolution of cybersecurity and supply-chain risk management practices in a manner that allows flexibility in addressing evolving threats. It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cybersecurity threats.

TBCP Grantee and Subgrantee Responsibility

Grantees and subgrantees that receive TBCP grants will be responsible for maintaining cyber and SCRM plans. We'll spend most of today discussing what the TBCP NOFO 2 requires of those plans and resources available to help Tribal Entities and subgrantees meet the requirements.

Tribal Entity Responsibility

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

What are the NOFO 2 Requirements for Cybersecurity?

TBCP NOFO 2 Cybersecurity Requirements

TBCP NOFO 2 Section F *pg. 61;* Each Eligible Entity is required to submit, as part of its TBCP application, an executed copy of the Certification Regarding Compliance with Cybersecurity and Supply Chain Management Requirements (Appx. A).

TBCP NOFO 2 Section F *pg. 62;* To accomplish the cybersecurity objectives of the United States Government, an Eligible Entity shall attest, and prior to allocating any funds to any subgrantee require it to attest, at a minimum, that it or they have completed the following actions:

Review the Cybersecurity and Critical Infrastructure Security Agency (CISA) **Cross-Sector Cybersecurity Performance Goals (CPGs).**

Perform an initial assessment of the cybersecurity practices of the TBCP award-funded project using the **CISA CPG Checklist Adapted for Grant Awards**. This assessment will include the cyber assets controlled as part of the execution of the project and the cybersecurity practices of the Eligible Entity organization and any subgrantees.

TBCP NOFO 2 Cybersecurity Requirements

Develop and submit a Cybersecurity Risk Mitigation Plan for the Eligible Entity organization and any **prospective or actual subgrantees** that includes:

- The **CISA CPG Checklist Adapted for Grant Awards** with a current assessment documented for cyber assets controlled as part of the project and assessment of the cybersecurity practices of the Eligible Entity organization and any prospective or actual subgrantees.
- A **prioritized list of the CPG gaps** for the project that need to be addressed for cyber assets controlled as part of the execution of the project, any CPG gaps affecting the Eligible Entity organization and any prospective or actual subgrantees.
- Documentation of project **cybersecurity risk mitigations** to be undertaken as part of execution of the grant award.

*An Eligible Entity also must ensure that, to the extent it or its subgrantee relies in whole or in part on network facilities owned or operated by a third party (e.g., purchases wholesale carriage on such facilities), it will obtain the above attestations from its network provider with respect to both cybersecurity and SCRM practices.

What are Eligible Uses of TBCP Funds for Cyber?

TBCP allows for the use of funds for cyber-related activities.

TBCP:

Eligible uses of funding in connection with Infrastructure Deployment activities include:

- Workforce Training
- Fund other allowable costs necessary to carrying out programmatic activities of an award, not to include ineligible costs

Eligible costs specific to Broadband Adoption and Use activities include:

- Provide digital training, education, technology support, outreach, and awareness programs including curricula and web-based resources
- Fund other allowable costs necessary to carrying out programmatic activities of an award, not to include ineligible costs

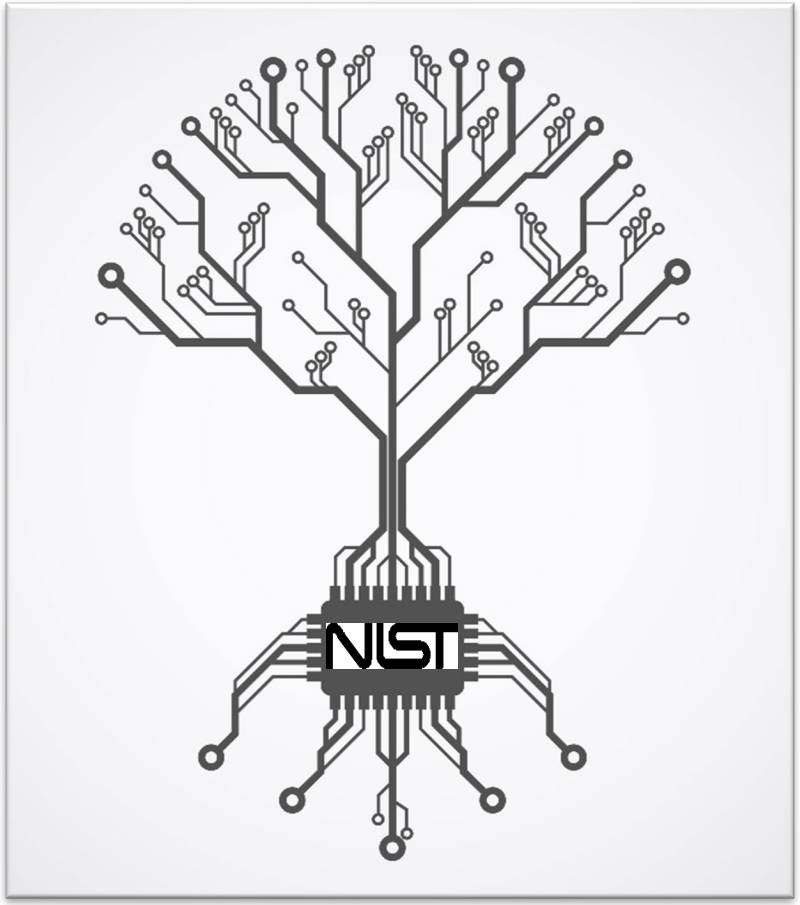
How Do I Develop a Cybersecurity Risk Management Plan?

Sample Profiles and Guidance

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

RESOURCES

- **TBCP Resource:**
  - Round two Appendix A Certification
- **CSF Resources:**
  - Risk Management Resources
  - Quick Start Guide
- **Communications-Specific Resources:**
  - 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 2 Requirements for Supply Chain Risk Management (SCRM)?

Supply Chain Risk Management (SCRM) Requirements

TBCP NOFO 2 Section F *pg. 61;* Each Eligible Entity is required to submit, as part of its TBCP application, an executed copy of the Certification Regarding Compliance with Cybersecurity and Supply Chain Management Requirements (Appx. A).

TBCP NOFO 2 Section F *pg. 62;* the Eligible Entity shall attest, and prior to allocating any funds to any subgrantee require it to attest, at a minimum, that:

The Eligible Entity and/or prospective subgrantee has a **SCRM plan in place** that is either: **operational**, if the Eligible Entity and/or prospective subgrantee is already providing service at the time of the grant; or **ready to be operationalized**, if the Eligible Entity and/or prospective subgrantee is **not yet providing service** at the time of grant award

The SCRM 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

Supply Chain Risk Management (SCRM) Requirements

The SCRM plan will be **re-evaluated and updated on a periodic basis** and as events warrant; and

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

*An Eligible Entity also must ensure that, to the extent it or its subgrantee relies in whole or in part on network facilities owned or operated by a third party (e.g., purchases wholesale carriage on such facilities), it will obtain the above attestations from its network provider with respect to both cybersecurity and SCRM practices.

What is Supply Chain Risk Management & How Do I Develop an SCRM Plan?

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

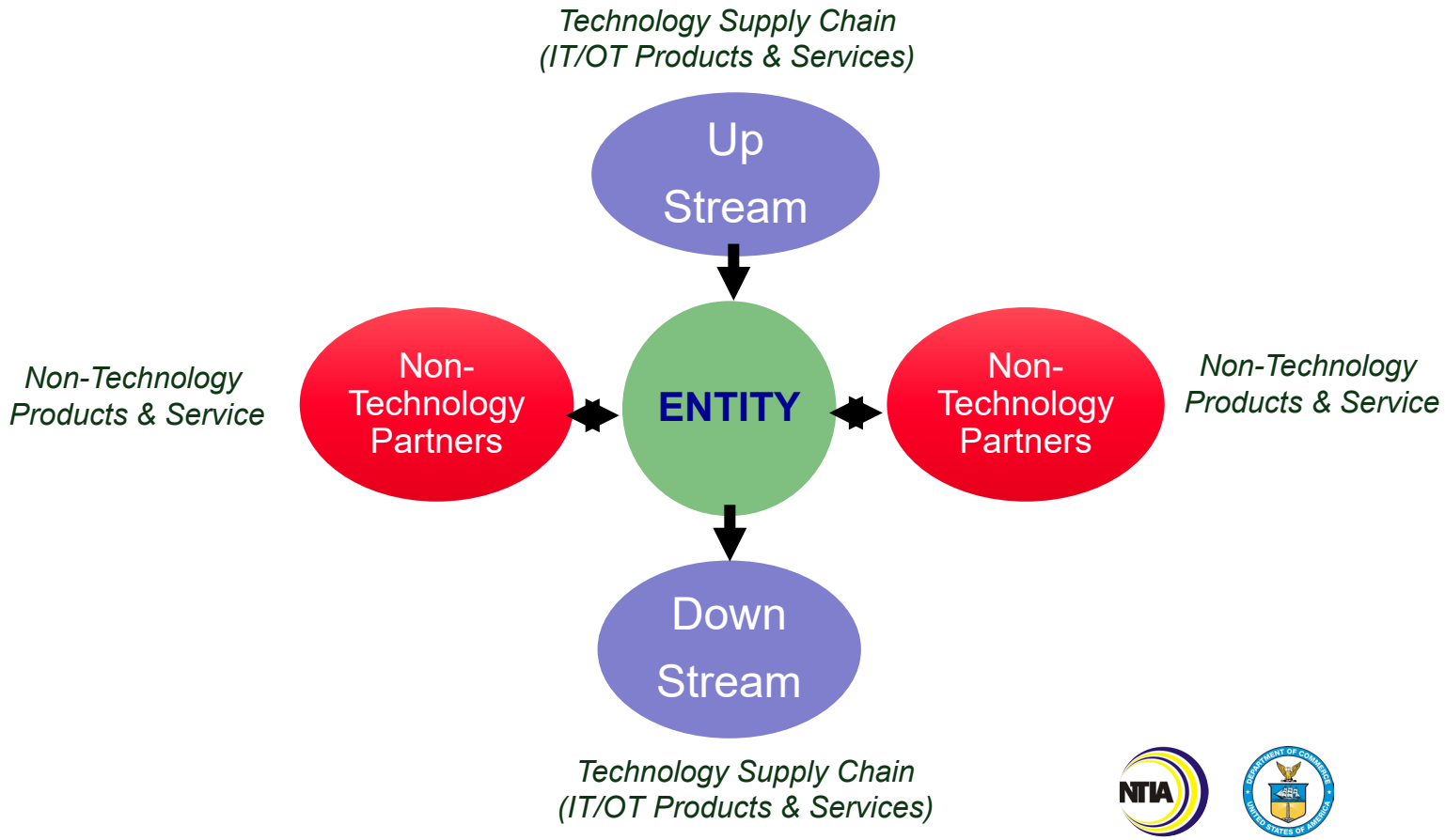
-Products/Service

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 Should Be Included in the SCRM Plan?

The SCRM 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 SCRM controls being implemented

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)*


INTERNET
FOR ALL
INTERNETFORALL.GOV

Q & A


NTIA


DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA


NTIA


DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA

Appendix – NIST Resources

What is the NIST Cybersecurity Framework (CSF)?

Cybersecurity Framework Attributes

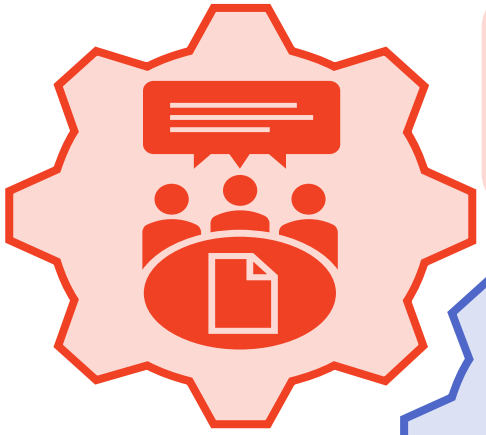
The NIST Cybersecurity Framework helps organizations reduce their cybersecurity risks and is widely recognized as foundational to securing organizations & technology.

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		
	Supply Chain Risk Management		
Protect (PR)	Identity Management & Access Control		
	Awareness and Training		
	Data Security		
	Information Protection Proces		
	Procedures		
	Maintenance		
	Protective Technology		
Detect (DE)	Anomalies and Events		
	Security Continuous Monitoring		
	Detection Processes		
Respond (RS)	Response Planning		
	Communications		
	Analysis		
	Mitigation		
	Improvements		
Recover (RC)	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

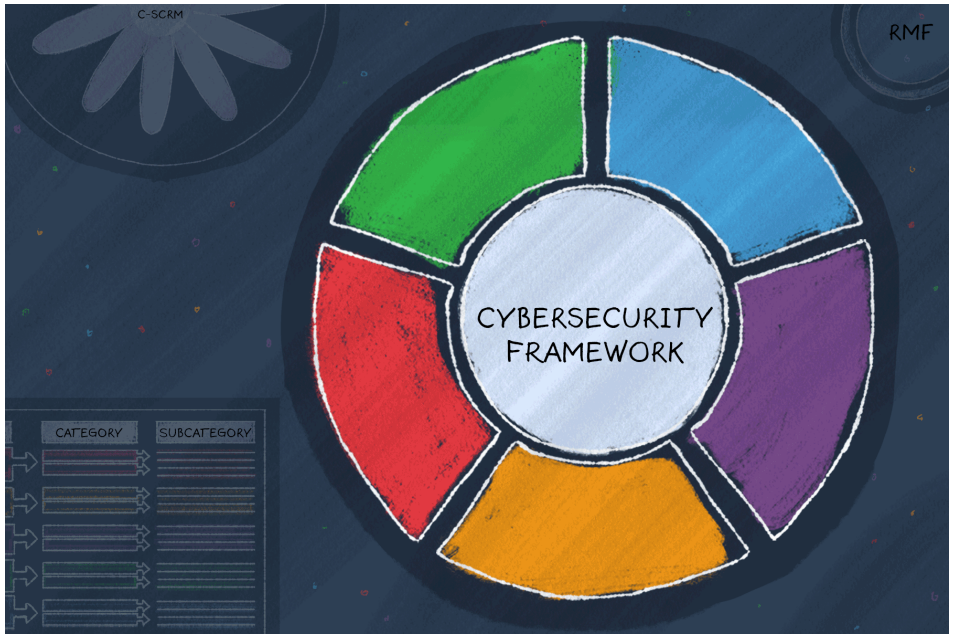
NIST continually updates the CSF to keep it up-to-date and accurate.

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 NIST Publication NISTIR 8276?

NISTIR 8276: Key Practices in C-SCRM

There are 8 key practices when using NISTIR 8276.

What is NIST 800-161? Rev.1

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

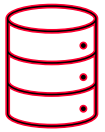
SP 800-161 Rev.1 provides guidance and tips for those creating supply chain risk management plans.

"Audience profiles and user guide"

Integrates C-SCRM into broader ERM activities & Across Layers of Organization

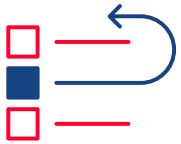
Guidance on development of a C-SCRM Program Management function

Adds Foundational, Sustaining, and Enhancing Key Practices

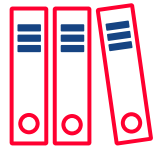


Modular Organization
- Main Body
- Multiple Appendices

Critical Success Factors:
- C-SCRM in Acquisition
- SC Information Sharing
- Training & Awareness
- Key Practices
- Measures and Measurement



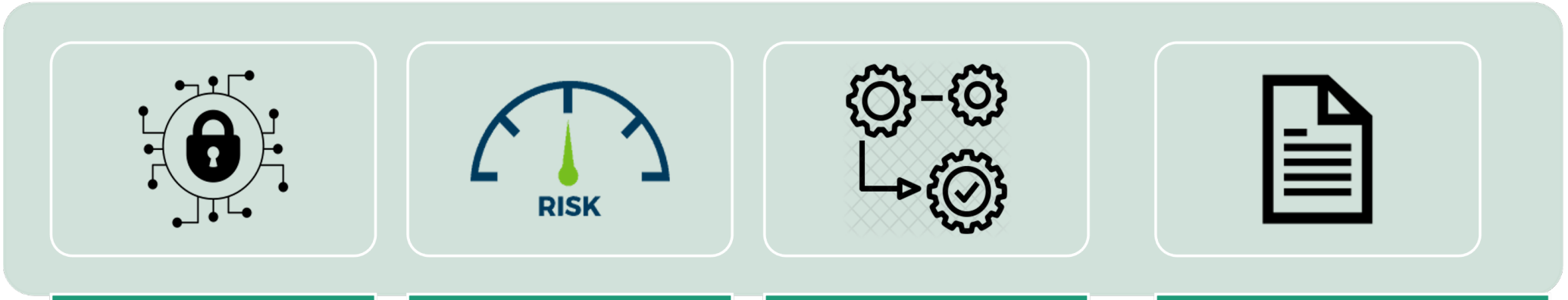
Appendix E on FASCSA and Appendix F on EO 14028 Section 4(d), Software Supply Chain Security



Updated & new references tables and graphics

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

A & B

Risk Exposure Framework

- Sample Risk Exposure Framework
- Threat Scenarios Examples

C

C-SCRM Activities in the Risk Management Process

- Describes Tasks for Each C-SCRM Process Step

G

Templates

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

D

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