



**National Institute of
Standards and Technology**
U.S. Department of Commerce

**NIST Workshop: Cyber Supply Chain Risk Management Practices for
Systems and Organizations (NIST Special Publication 800-161,
Revision 1), Initial Public Draft**

Draft NIST SP 800-161

Rev 1 Drafting Team

Computer Security Division

IT Laboratory

12 May 2021



REMINDER: Submit any questions through Q&A during this workshop. Questions will be answered at the end of the workshop.

Agenda

Introduction and purpose of the workshop – 10 min

Overview of NIST SP 800-161 Revision 1 – 45 min

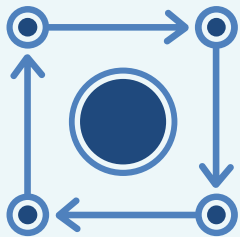
Submitted Q&A Discussion – 30 min

Open Q&A – 15 min

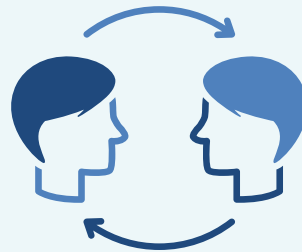
Wrap up – 5 min

Introduction and Purpose of the Workshop

NIST C-SCRM guidance has been designed to help organizations to identify, assess, and respond to cyber supply chain risks. The purpose of this workshop is to:



Provide
overview
of major
changes



Engage
stakeholders
to obtain
comments
and opinions



Provide
clarity of
intent based
on submitted
questions

Intention and Approach to Drafting Revision

Since original publication in 2015

- Managing risks associated with acquiring products and services continues to be a concern
- Legislation, regulations, and policies have changed
- Federal and industry practices have evolved

Why do we have new content

- Provide relevant information to different types of stakeholders - e.g., program management office (PMO), systems engineers, system security engineers, procurement officer, maintenance engineer, delivery organization and acceptance engineers, system integrators
- Increase use by industry stakeholders
- Capture leading C-SCRM practices from government and industry
- Integrate new concepts and processes that emerged since original publication, incorporated into other NIST guidance (e.g., SP 800-37 Rev 2, SP 800-53 Rev 5, SP 800-53B)
- Provide additional tools and guidance to organizations that are just getting started, e.g., how to develop a PMO, key practices, and templates

Major Changes in Draft Revision



Adds Foundational, Sustaining, and Enhancing Key Practices



Integrates C-SCRM into broader ERM activities; includes NextGen C-SCRM controls



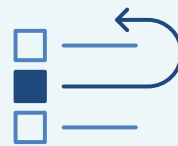
Provides guidance on development of PMO function



Addresses Critical Success Factors



Includes templates



Updates Risk Exposure Scenario: includes FOCI



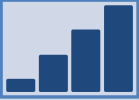


Includes updated or new references tables and graphics



Increases usability to more audiences

Key Practices

Implementation Level	Associated C-SCRM Practices
Foundational 	<ul style="list-style-type: none">• PMO• Strategy and Policies• Identified critical components and suppliers• Integrated into acquisition
Sustaining 	<ul style="list-style-type: none">• Clearly defined risk appetite and risk tolerance• Use of a formalized info sharing process to engage with other Federal D/As• Formal C-SCRM Training, stand-alone and integrated with training on other topics (e.g., cybersecurity or safety)• Collaboration with suppliers to help them improve their cybersecurity and C-SCRM practices• Collection and reporting of qualitative C-SCRM metrics
Enhancing 	<ul style="list-style-type: none">• Automated C-SCRM processes• Quantitative risk analysis• Use of forward-leaning quantitative C-SCRM metrics

Greater integration with ERM (I/IV)

- Tighter linkages to relevant NIST publications for
 - Overall C-SCRM process – SPs 800-39
 - SCRM Plan and ATO processes – (800-37r2)
 - C-SCRM controls – 800-53r5
 - Baselines – 800-53B
- Risk Management roles & responsibilities and activities within multiple organizational levels – Enterprise (1), Mission/Business Process (2), and Operational (3)
- Critical Success Factors
 - Establish acquisition processes
 - Implement information sharing
 - Provide C-SCRM awareness and training
 - Implement C-SCRM Metrics
 - Deploy dedicated resources

Greater integration with ERM (II/IV)

- Guidance on development of a dedicated PMO function
 - Defines scope and characteristics of a C-SCRM Program across organizational levels
 - Codifies C-SCRM PMO's purpose, high level roles, and scope of responsibilities
 - Discusses application of PMO within and across organizational levels, especially where responsibilities may overlap
 - Outlines flexible models (e.g., centralized, decentralized, hybrid with dedicated or matrixed representatives) for PMOs
 - Identifies beneficial services a PMO may provide

Greater integration with ERM (III/IV)

- Offers Guidance in Appendix C, C-SCRM Activities in the Risk Management Process
 - Integrating C-SCRM into the acquisition process
 - Providing enhanced overlay of C-SCRM into the SP 800-39 Risk Management Process
- Combines two complementary risk management approaches to facilitate risk management across 3 levels
 - FARM: Frame, Assess, Respond, Monitor (levels 1&2)
 - Risk Management Framework: Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor (level 3)

Greater integration with ERM (IV/IV)

Defines Activities

- 1-1: Risk assumptions
- 1-2: Risk management process constraints
- 1-3: Risk appetite and tolerance
- 1-4: Priorities and trade-offs
- 2-1: Threat and vulnerability identification
- 2-2: Risk determination
- 3-1: Risk response identification
- 3-2: Evaluation of alternatives
- 3-3: Risk response decision
- 3-4: Risk response implementation
- 4-1: Risk monitoring strategy
- 4-2: Risk monitoring

C-SCRM Enablement through Templates

- Strategy and Implementation Plans
- Policies
- Plans
- Product/Service and Supplier Assessments


Improved usability of document

- Different user groups were kept in mind
- Linkages or references to related parts of the document are provided
- Main document contains high-level guidance (e.g., introduction, Integration into risk management, critical success factors, C-SCRM implementation guidance)
- Appendices provides processes and tools (e.g., templates, risk response framework scenarios) or reference materials (e.g., control summary matrix, acronyms, references, definitions)
- SP 800-53 Rev5 controls were removed from this Revision as they are available separately

Request for Feedback from Reviewers – General Questions

- Does this guidance offer organizations a structure both easy to follow and implement? If not, how could it be improved?
- Is there any additional guidance or tools (e.g., templates) that should be included?
- What else may be missing that would be helpful to include?
- Is there anything missing from Critical Success Factors to include C-SCRM Strategy and Implementation Plan, or the role of C-SCRM in the acquisition process?
- Is there a different approach preferred that is not currently reflected by the C-SCRM Practice Implementation Model (Foundational, Sustaining, Enhancing)?
- What can improve the product or service assessment (Appendix D, 4.1 Cyber Supply Chain Risk Assessment Template)?

Notional Timeline: Dates Subject to Change

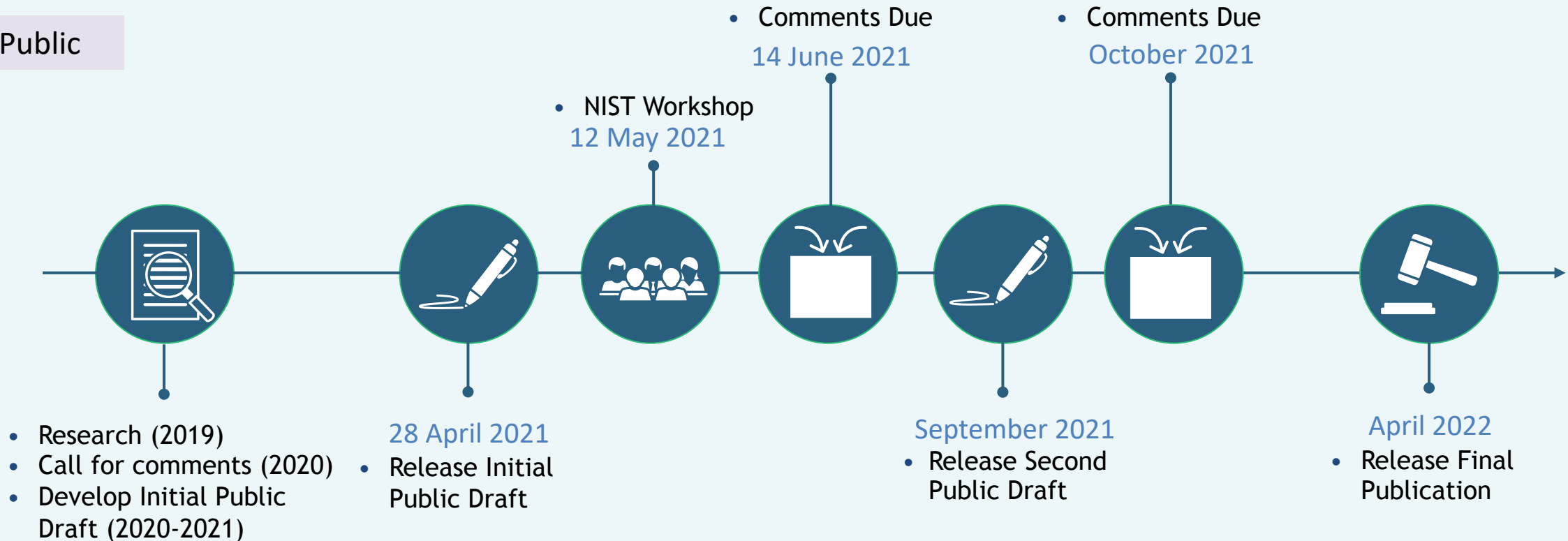
 We are here

2019/2020

2021

2022

Public



Internal R&D

Open "Live" Q&A



Questions submitted via Q&A during the workshop will be answered during this time

Wrap up



Thank
you!!



And HONK
if you
support
C-SCRM

Email: scrm-nist@nist.gov

Visit: <http://scrm.nist.gov>