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

NIST Workshop: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST Special Publication 800-161, Revision 1), 2nd Public Draft

Draft NIST SP 800-161
Rev 1 Drafting Team
Computer Security Division
IT Laboratory

1 December 2021

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

Agenda

Part 1:

Introduction and purpose of the workshop – 5 min

Overview Changes to 2nd Public Draft of NIST SP 800-161 Revision 1 – 10 min

Overview of New FASCSA Section (Appendix E) – 10 min

Overview of Response to EO 14028 (Appendix F) – 10 Min

Submitted Q&A Discussion – 10 min

Part 2:

Panel Discussion – 45 Min

Changes to the 2nd Public Draft of NIST SP 800-161 Rev. 1:

2nd Public Draft Major Changes and Updates (I/II)[1]

Major Changes:
- Added C-SCRM metrics development process
- Updated Risk Appetite & Tolerance discussion and moved to Appendix G
- Collapsed Section 4
- Added Appendix E – FASCSA Discussion
- Added Appendix F – Response to EO 14028

Section 1:
- Added Audience Profiles and Document Use Guidance
- Added contrast between terms "enterprise" and "organization" to align with NISTIR 8286
- Added discussion of tailoring C-SCRM
- Revised dimensions of C-SCRM (flower graphic)

Section 2:
- Imported from Section 1 – The Business Case for C-SCRM
- Imported from Section 1 – Cybersecurity Risks in Supply Chains
- Revised and streamlined Multi-Level Risk Management discussion

Section 3:
- Imported from Section 1 – C-SCRM Key Practices; added additional practices
- Added Section 3.5.1, Measuring C-SCRM Through Performance Measures

2nd Public Draft Major Changes and Updates (II/II)[1]

Appendix A: C-SCRM Controls
- Imported from Section 4 – C-SCRM Controls
- Added discussion of EO 14028 related topics

Appendix C: Risk Response Framework
- Added Scenario 6 on Vulnerable Reused Components within Systems

Appendix D: C-SCRM Templates
- Added References to EO 14028

Appendix E: FASCSA
- New section providing additional guidance to specific to federal agencies related to FASCSA

Appendix F: Response to Executive Order 14028's Call to Publish Preliminary Guidelines for Enhancing Software Supply Chain Security
- New section providing a response to EO 14028's directive to establish preliminary guidelines for enhancing software supply chain security

Appendix J: References
- Imported from Section 1 – Relationship to Other Programs and Publications
- Imported from Section 1 – Implementing C-SCRM in the context of SP 800-37 Rev. 2
- Imported from Section 1 – Methodology for Building C-SCRM Guidance Using SP 800-39, SP 800-37 Rev. 2, and SP 800-53 Rev.5

Appendix E: FASCA

Federal Acquisition Supply Chain Security Act of 2018 (Title II of SECURE Technology Act)

- Established the Federal Acquisition Security Council
- Provides legal authorities relating to mitigating supply chain risks in the procurement of information and communications technology and services.
- Requires federal agencies perform supply chain risk management/risk assessments
- Agencies are to use NIST standards/guidance when assessing and developing mitigation strategies to address supply chain risks

Appendix Overview

- Audience is Federal Executive Branch Agencies
- Guidance pertains to FASCSA Section 1326 (a) requirements – all agencies are to conduct supply chain risk assessment (SCRA) and prioritize those assessments
- Agencies are to perform SCRAs, and other SCRM activities described in the law, consistent with NIST standards, guidelines, and practices.
- This guidance was informed by lessons learned, research and engagement with industry and the interagency, FASC rule and process requirements, input from SMEs.
- Appendix includes note to clarify difference and relationship between supply chain risk definitions
- FASCSA definition is focused on adversarial risk
- NIST cybersecurity supply chain risk definition is broader and inclusive of FASCSA definition but also encompasses non-adversarial threats/risks.

Baseline Risk Factors

Factors are:

- Inclusive of both adversarial and non-adversarial risks
- Consistent with and align to the factors included in the FASC rule
- Grouped into two broad categories:
- Context = Inherent Risk
- Supply-side Threats/Vulnerabilities = Inherited Risk

Baseline = Common, Minimal Factors

- Required for all critical suppliers (i.e., sources); critical services, critical systems or system components and
- Required if/when a risk associated with a source/covered article is determined to be substantial
- Agency has discretion to use for all other suppliers, services, products
- Agencies should augment/tailor factors to their specific use case.

Supply Chain Risk Severity Schema

Level	Type	Description
5	Urgent National Security Interest Risk	Adversarial-related significant risk with imminent or present impact to National Security Interest
4	National Security Interest Risk	Adversarial-related significant risk with potential to impact National Security Interest
3	Significant Risk	Adversarial-related significant risk assessed, with potential or known multi-agency/ mission(s) or Government-wide impact
2	Agency High Risk	Adversarial or non-adversarial-related risk associated with a critical supplier (i.e., source), critical system or asset, or critical system component, and assessed to have a risk that is high, per agency-established risk level assessment. Assessed risk impact does not extend outside of the agency.
1	Agency Low or Moderate Risk	Adversarial or non-adversarial risk is assessed which falls within agency's risk tolerance/appetite thresholds. Assessed risk impact does not extend outside of the agency.

"Substantial Risk"

"Escalate Internally; Potential for being Substantial Risk"

Documentation

- Purpose is to communicate expectations about what information needs to be included in an assessment “record”
- It establishes a robust and defensible record to underpin an agencies’ review of risk and subsequent escalation processes and risk response decisions and actions.
- It also helps to promote consistency in the scope and organization of documented content to facilitate comparability, re-usability, and information sharing.

Appendix F:

Response to Executive Order 14028's Call to Publish Preliminary Guidelines for Enhancing Software Supply Chain Security

Appendix F

Section 4 (c) *Within 180 days of the date of this order, the Director of NIST shall publish preliminary guidelines, based on the consultations described in subsection (b) of this section and drawing on existing documents as practicable, for enhancing software supply chain security and meeting the requirements of this section.*

Approach

- Use existing industry standards, tools, and recommended practices sourced from the main body of draft SP 800-161 Revision 1.
- Use previous guidance published by NIST as a result of the EO, including:
  - **Definition of Critical Software** Under Executive Order (EO) 14028; June 25, 2021
  - **Security Measures for "EO-Critical Software"** Use Under Executive Order (EO) 14028; July 9, 2021
  - **Guidelines on Minimum Standards for Developer Verification** of Software; July 2021
- New standards, tools, and recommended practices sourced from over 150 position papers stemming from Section 4 (b) workshop in June 2021.
- Other related software supply chain-related work in the EO
- Foundational, Sustaining, Enhancing

Appendix F…continued

- Security Measures for EO-Critical Software
  - Recommend flowing down controls to suppliers
- Guidelines on Minimum Standards for Developer Verification
  - Developed a chart where verification techniques can be used as part of various C-SCRM controls
- NOT IN THIS DRAFT: Section 4 (e) Secure Software Development Framework (TBD)
- Cybersecurity Labeling for Consumers: IoT Devices and Software
  - FISMA is applicable to IoT so applicable security measures should be already in place
  - NISTIR 8259 *Recommendations for IoT Device Manufacturers: Foundational Activities* as well as NISTIR 8259A *Core Device Cybersecurity Capability Baseline*
  - CISA's *Internet of Things Acquisition Guidance*
  - *NOT IN THIS DRAFT: Draft SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government* (TBD)
- Emerging software supply chain concepts (Foundational, Sustaining, Enhancing)
  - Software Bill of Materials (SBOM)
  - Enhanced Vendor Risk Assessments
  - Open Source Software Controls
  - Vulnerability Management Practices
- Existing Industry Standards, Tools, and Recommended Practices

Submitted Q&A Discussion

Panel Discussion on Appendix F / EO 14028 Section 4(c)

Panelists

Valecia Maclin
Microsoft

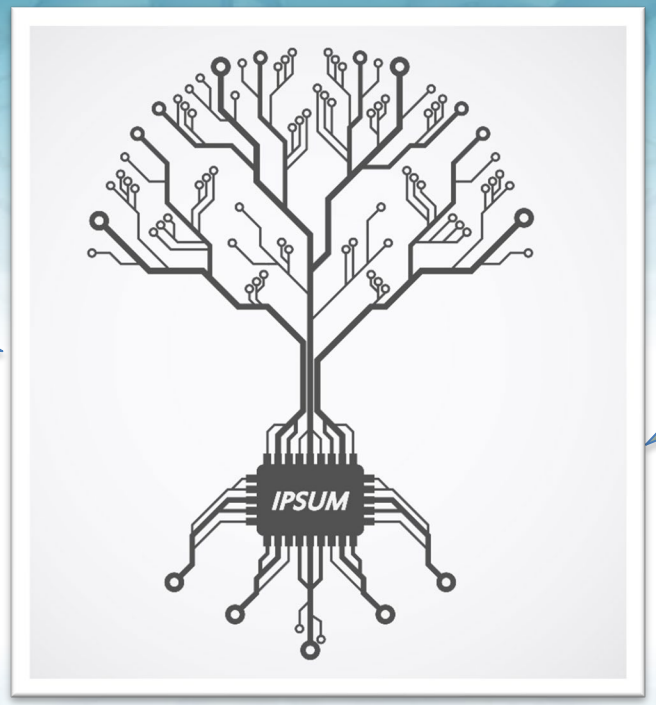
John Nuckles
IC SCC

Nathanael Paul
Dexcom

Moderator

Matthew Fallon
BCG

Thank you!!



And HONK if you support C-SCRM

Email: scrm-nist@nist.gov

Visit: http://scrm.nist.gov