Cyber - Supply Chain Risk Management in NIST Publications

Celia Paulsen
11/13/2019
NIST Labs and Extramural Programs

- Material Measurement Laboratory
- Physical Measurement Laboratory
- Engineering Laboratory
- Information Technology Laboratory
- Communication Technology Laboratory
- Center for Nanoscale Science and Technology
- NIST Center for Neutron Research
- Hollings Manufacturing Extension Partnership
- Manufacturing USA
- Baldrige Performance Excellence Program

11/13/2019
Agenda

- NIST SP 800-37 Rev. 2
- NIST SP 800-171 series
- DRAFT NIST SP 800-53 Rev. 5
- NIST SP 800-161

Framework for Improving Critical Infrastructure Cybersecurity
Agenda

1. NIST SP 800-37 Rev. 2
2. NIST SP 800-171 series
3. DRAFT NIST SP 800-53 Rev. 5
4. NIST SP 800-161

Framework for Improving Critical Infrastructure Cybersecurity
Update:

- Integrates privacy, **supply chain**, and security engineering into the Risk Management Framework (RMF)
- Aligns the Cybersecurity Framework to the RMF
- Demonstrates how the RMF is implemented in the system development life cycle

**New Step: Prepare**

- All RMF Tasks include potential inputs and expected outputs
- ‘New’ Tasks in existing Steps
RMF & C-SCRM

• Guidance is in alignment with FISMA and OMB A-130 requirements

• Every step in the RMF can **(not necessarily should)** be executed by nonfederal external providers **except** for the **Authorize** step

**Chapter 2.8:**

• Introduction to supply chain risk

• Directs organizations to **develop a SCRM policy** similar to a Risk Management Strategy (Task P-2):
  • Supports other organizational policies (e.g. acquisition, information security)
  • Addresses **goals and objectives**
  • Defines **integration points** for SCRM with other organizational activities
  • Defines **roles and responsibilities**
  • Describes (briefly) how organizations obtain assurance from providers
RMF & C-SCRM (Tasks)

C-SCRM additions to Tasks:

• **Throughout:** “including supply chain risks”

• **Task P-3:** *Integrate supply chain risk assessment results* into the organization-wide risk assessment

• **Task P-7:** Include supply chain risk considerations in organizational continuous monitoring strategies

• **Task P-9:** *Identify stakeholders* (including through all aspects of the supply chain)

• **Task P-11:** For systems partially or wholly managed, make sure the **authorization boundary is clearly defined in agreements.**
RMF & C-SCRM (Tasks)

• **Task P-14:** Conduct a *system-level supply chain risk assessment*
  • Risk that the *use of an external provider* could result in loss
  • Risk related to the *disposition of a system/elements*
  • **Collaborate with supply chain partners** on assessments/mitigations

• **Task P-15:** Consider supply chain when making *security requirements*

• **Task C-1:** Include supply chain information (i.e. provenance) in *system description*

• **Task A-2:** If a third party is involved in implementing controls, the organization can *request the assessment plan / results / evidence* (may require contract or NDA)

• **Task A-3:** Assessments can be conducted on commercial products
For More on NIST SP 800-37 Rev. 2:


- Video and presentations from “RMF 2.0” webcast: [go.usa.gov/xENcs](go.usa.gov/xENcs)


- NIST RMF Team: sec-cert@nist.gov
Agenda

11/13/2019

NIST SP 800-37 Rev. 2

NIST SP 800-171 series

DRAFT NIST SP 800-53 Rev. 5

NIST SP 800-161

Framework for Improving Critical Infrastructure Cybersecurity
Executive Order 13556: established government-wide CUI program

CUI Registry:
- information, guidance, policy, and requirements on handling CUI
- identifies approved CUI categories and sub-categories
- Sets out procedures for the use of CUI (marking, safeguarding, transporting, etc.)

NIST SP 800-171 Rev. 1: Provide federal agencies a set of recommended security requirements for protecting the confidentiality of Controlled Unclassified Information (CUI) in nonfederal systems and organizations

NIST SP 800-171A: Provides federal and nonfederal organizations with a methodology that can be employed to conduct assessments of the CUI security requirements in NIST SP 800-171.

NIST SP 800-171B (DRAFT): Provides enhanced security requirements where information runs a higher than usual risk of exposure, when mandated in a contract, grant, or other agreement.
Assumptions re: Nonfederal Organizations

- Have information technology infrastructures in place.
  - Are not developing or acquiring systems specifically for the purpose of processing, storing, or transmitting CUI.

- Have safeguarding measures in place to protect their information.
  - May also be sufficient to satisfy the CUI requirements.

- May not have the necessary organizational structure or resources to satisfy every CUI security requirement.
  - Can implement alternative, but equally effective, security measures.

- Can implement a variety of potential security solutions.
  - Directly or through the use of managed services.
For more on the NIST SP 800-171 series

Publications:
• 800-171A: https://csrc.nist.gov/publications/detail/sp/800-171a/final
• 800-171B: https://csrc.nist.gov/publications/detail/sp/800-171b/draft

Other:
• Video and presentations from October 2018 workshop: https://www.nist.gov/news-events/events/2018/10/controlled-unclassified-information-security-requirements-workshop

• NIST CUI website with FAQ: https://csrc.nist.gov/Projects/protecting-controlled-unclassified-information

• NIST RMF Team: sec-cert@nist.gov
Agenda

11/13/2019

NIST SP 800-37 Rev. 2
NIST SP 800-171 series
DRAFT NIST SP 800-53 Rev. 5
NIST SP 800-161

Framework for Improving Critical Infrastructure Cybersecurity

NIST SP 800 series
NIST SP 800-171 series
DRAFT NIST SP 800-53 Rev. 5
NIST SP 800-161

NIST Special Publication 800-37
Risk Management Framework for Information Systems and Organizations
A System Life Cycle Approach for Security and Privacy

NIST Special Publication 800-171 series
Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

NIST Special Publication 800-53
Draft NIST Special Publication 800-53
Security and Privacy Controls for Information Systems and Organizations

NIST Special Publication 800-161

NIST Special Publication 800-143
Computer Security

Framework

RECOVER
IDENTIFY
PROTECT
RESPOND
DETECT
Security (and now Privacy) control catalog

**Update** *(NOT ALL ARE IN THE PUBLISHED DRAFT):*

- Reduced federal focus
- Align with other publications (SP 800-161, SP 800-160, CSF)
- Decoupled “information” from “system”
- Separate control selection process from the controls themselves
  - Information will be moved to other NIST publications (e.g. SP 800-37)
- Removed tailoring guidance to appendix
- Incorporate new state-of-the-practice controls
- Established *new supply chain risk management family*

- Future update may involve transitioning controls to an online portal
New supply chain risk management family (SR family)
  • Moved SA-12 into the new family
  • SCRM Policy
  • System-level SCRM Plan concept from NIST SP 800-161
  • Provenance concept from NIST SP 800-161

PM-31 Supply Chain Risk Management Strategy
  • Is the organization-level SCRM plan from SP 800-161

RA-3(1) Supply Chain Risk Assessment

IR-family: reporting of supply chain incident information and coordinating with supply chain partners

Throughout: AT-3 role-based training; CM-4 impact analysis, MA-2 controlled maintenance; SC-29 Heterogeneity, etc.
For more on the NIST SP 800-53

Publications:


• Published Draft 800-53 Rev. 5 (as of Aug. 2007):

• Website: https://csrc.nist.gov/Projects/risk-management

• NIST FISMA Team: sec-cert@nist.gov
The C-SCRM flagship document

Used familiar publications to demonstrate how federal departments and agencies could integrate C-SCRM into their existing processes.

- **Tiered** risk management from NIST SP 800-39
- **Risk Assessment** methodology from NIST SP 800-30 (Frame, Assess, Respond, Monitor)
- **Security controls** from NIST SP 800-53 Rev. 4

- 6 new controls and/or control enhancements (not in NIST SP 800-53 Rev 4)
- New control family – “Provenance”
C-SCRM Practices

Update beginning this FY:
• Align with NIST SP 800-53 Rev. 5 (and other documents)
• Provide additional implementation guidance
• Add additional controls

• Provides a resource for people **focused** on SCRM
• Directed towards **federal departments and agencies**, but the information may be usable by any organization

**Trust**
- Organization
- Process
- Products/Service

**But Verify**
- Due Diligence
- Audits
- Testing
For more on the NIST SP 800-161

• Publication: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

• Software and Supply Chain Assurance Forum: https://csrc.nist.gov/scrm/ssca

• NIST SCRM Webpage: https://csrc.nist.gov/scrm

• NIST SCRM Team: scrm@nist.gov
Agenda

- NIST SP 800-37 Rev. 2
- NIST SP 800-171 series
- NIST SP 800-161
- DRAFT NIST SP 800-53 Rev. 5

Framework for Improving Critical Infrastructure Cybersecurity
Voluntary framework:

• Core: cybersecurity activities and outcomes
• Implementation Tiers: context on how an organization views cybersecurity
• Profiles: an organization’s unique alignment against the Framework Core

Version 1.1:

• Section 3.3: expanded to discuss SCRM
• Section 3.4 (new): buying decisions
• SCRM criteria added to implementation tiers
• Added a Supply Chain Management Category (ID.SC)
• Also has other subcategories that are SCRM-related

--Communication Tool--
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Business Environment (ID.BE): …</td>
<td>ID.BE-1: The organization’s <strong>role in the supply chain</strong> is identified and communicated</td>
</tr>
<tr>
<td></td>
<td>Supply Chain Risk Management (ID.SC): …</td>
<td>ID.SC-1: <strong>Cyber supply chain risk management processes</strong> are identified, established, assessed, managed, and agreed to by organizational stakeholders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.SC-2: <strong>Suppliers and third party partners</strong> of information systems, components, and services are <strong>identified, prioritized, and assessed</strong> using a cyber supply chain risk assessment process</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.SC-3: <strong>Contracts</strong> with suppliers and third-party partners are <strong>used to implement appropriate measures</strong> designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.SC-4: Suppliers and third-party <strong>partners are routinely assessed</strong> using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.SC-5: <strong>Response and recovery</strong> planning and testing are conducted with suppliers and third-party providers</td>
</tr>
<tr>
<td>Protect</td>
<td>Awareness and Training (PR.AT): …</td>
<td>PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their <strong>roles and responsibilities</strong></td>
</tr>
</tbody>
</table>

---

**CSF & C-SCRM**

11/13/2019

24
For more on the CSF

• Website: https://www.nist.gov/cyberframework

• CSF Roadmap 1.1: https://www.nist.gov/cyberframework/related-efforts-roadmap

• CSF Team: cyberframework@nist.gov
Questions?

Risk Management Team
Sec-cert@nist.gov

Celia Paulsen
celia.paulsen@nist.gov

C-SCRM Team
csrc.nist.gov/scrm
scrm@nist.gov