From: **Dan Reddy**
Date: Sun, Apr 9, 2017 at 8:03 PM
Subject: NIST CSF 1.1 Comments
To: cyberframework@nist.gov
Cc: Jon M Boyens

Please find a pdf with detailed sticky notes comments to CSF 1.1. Please let me know if you have any trouble reading them.

[Sticky Notes Below]

Note to Reviewers on the Update and Next Steps
• Good choice on compatibility with 1.0
• Consider adding Cyber SCRM to your Glossary

Is there a better label than "version 1.1" for this update?
• 1.1 is fine for the name

Framework Implementation Tiers
• Tier has always been an interesting choice. I knew that you don't want to hint at maturity. Tier is at a least neutral word but has always been a bit odd. Did you get other reactions to Tiers? Probably too late to change. I'd have done "Levels"

Framework Profile
• Profile are a great concept. Can enable lots of supplemental work.

Section 2.2 Framework Implementation Tiers
• Line 349
• Again I get that you don't want to do "maturity levels". Below you indicate that one Tier or another might reflect your Risk Tolerances. Who in critical infrastructure would really want to stay in Partial as a desired end state? Doesn't hold water with me.

Section 2.2 Framework Implementation Tiers
• Tier 3: Repeatable "Cyber Supply Chain Risk Management"
• While you know that I' SCRM fan, it does appear that you're devoting lots of Tier text to C-SCRM. Will you get push back?

Section 2.2 Framework Implementation Tiers
• Line 440 "External Participation"
• Some overlap with the following next C- SCRM

Section 2.2 Framework Implementation Tiers
• Line 442 "…before a cybersecurity event occurs."
• What about relationships during responses to events?

Section 3.0 How to Use the Framework
• Line 449 "…business partners and customers…"
• add "suppliers"

Section 3.0 How to Use the Framework
• Lines 502-503 "The Framework can be applied in design, build/buy, deploy, operate, and decommission system lifecycle phases."

• Yes the CSF can be Applied to system lifecycle phases but it's not a perfect alignment with an SDL. It does have useful ingredients that can be leveraged with a lifecycle. Your examples help but you wouldn't want someone to go too far with it. This area needs more guidance. I need to spend more time with 160.

Section 3.2 Establishing or Improving a Cybersecurity Program

• Lines 543 – 544 “Implementation Tiers may be used to express varying risk tolerances.”
• See above note on people not really Deciding that Partial is a appropriate place to be. Makes a bit more sense with upper tier differences.

Section 3.2 Establishing or Improving a Cybersecurity Program

• Lines 564 – 566
• Again would you choose the characteristics of Partial?

Section 3.3 Communicating Cybersecurity Requirements with Stakeholders

• Lines 601 – 625
• Again seems like this section has lots of C-SCRM content for a generic section. As you know I'm biased but had to point it out.

Section 3.3 Communicating Cybersecurity Requirements with Stakeholders

• Line 628 “…Buyer…”
• Is Buyer defined?

Section 3.4 Buying Decisions

• A Buying Decisions section does deserve more C-SCRM focus

Section 3.7 Federal Alignment

• If you're creating a Federal Alignment section should you explicitly mention Commercial l Alignment where no major Federal role exists and Federal standards may not apply. Commercial best practices that apply to COTS ICT cyber assets are more appropriate. Mention COTS ICT like OTTPS (ISO 20243) and Implementation Guide from Open Group. Quote Guide and put footnote.

Section 4.0 Measuring and Demonstrating Cybersecurity

• Lines 750 – 755
• I bet I know who wrote this!

Section 4.1 Correlation to Business Results

• Line 799 “Enterprise risk management…”
• Speaking of Enterprises and C-SCRM, are there any references to extended enterprises through cloud or other managed services that deserve a mention?

Section 4.2 Types of Cybersecurity Measurement

• Line 832
• Good to include For instances. helps to keep this from being too theoretical

Appendix A: Framework Core

• Lines 865 – 866
• Should include ISO 20243 for COTS ICT for anti counterfeit and tampered

Table 2: Function and Category Unique Identifiers

• ID.SC Supply Chain Risk Management
• I can see SCRM being anchored in one Function and Identify has other items that are a bit global.

Table 3: Framework Core

• ID.AM-1

NIST CSF Subcategory
O-TTPS Attribute/ Requirement
O-TTPS Description
ID.AM-1: Physical devices and systems within the organization are inventoried.
4.1.1.5 PD_PSM: Product Sustainment Management
Product support, release maintenance, and defect management are product sustainment services offered to acquirers while the product is generally available.

Table 3: Framework Core

• ID.AM-2

NIST CSF Subcategory
O-TTPS Attribute/ Requirement
O-TTPS Description
ID.AM-2: Software platforms and applications within the organization are inventoried.
4.1.1.5 PD_PSM: Product Sustainment Management
Product support, release maintenance, and defect management are product sustainment services offered to acquirers while the product is generally available.

Table 3: Framework Core

• ID.AM-6

NIST CSF Subcategory
O-TTPS Attribute/ Requirement
O-TTPS Description
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.
4.2.1.1 SC_RSM: Risk Management
The management of supply chain risk around tainted and counterfeit components and products includes the identification, assessment, prioritization, and mitigation of corresponding business, technical, and operational risks

Table 3: Framework Core

• ID.BE-1

NIST CSF Subcategory
O-TTPS Attribute/ Requirement
O-TTPS Description
ID.BE-1: The organization's role in the supply chain is identified and communicated.
4.2.1.5 SC_BPS: Business Partner Security
Relevant business partners follow the recommended supply chain security best practice requirements specified by the O-TTPS. Periodic confirmation is requested that business partners are following the supply chain security best practice requirements specified by the O-TTPS.

Table 3: Framework Core

• ID.GV-2

NIST CSF Subcategory
O-TTPS Attribute/ Requirement
O-TTPS Description
ID.GV-2: Information security roles and responsibilities are coordinated and aligned with internal roles and external partners.
4.2.1.5 SC_BPS: Business Partner Security
Relevant business partners follow the recommended supply chain security best practice requirements specified by the O-TTPS. Periodic confirmation is requested that business partners are following the supply chain security best practice requirements specified by the O-TTPS.

Table 3: Framework Core

• ID.GV-3

NIST CSF Subcategory
O-TTPS Attribute/ Requirement
O-TTPS Description
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
4.2.1.5 SC_BPS.02: Business Partner Security

Legal agreements with business partners should reference applicable requirements for supply chain security practices (e.g., O-TTPS).

Table 3: Framework Core

• ID.RA-1

NIST CSF Subcategory
O-TTPS Attribute/ Requirement
O-TTPS Description
ID.RA-1: Asset vulnerabilities are identified and documented.
4.1.2.3 SE_VAR.03: Vulnerability Analysis and Response
A process shall exist for governing notification of newly discovered and exploitable product vulnerabilities.
4.1.1.5 PD_PSM.02: Product Sustainment Management
Release maintenance shall include a process for notification to acquirers of product updates.

Table 3: Framework Core

• Supply Chain Risk Management (ID.SC)

• OTTPS (ISO/IEC 20243) should be added as a Informative reference. The developers of OTTPS over 7 years have used these practices more that people have gone to 27001 for supply chain guidance. How many orgs have been audited for SCRM 27001?

Table 3: Framework Core

• PR.AC-1

NIST CSF Subcategory
O-TTPS Attribute/ Requirement
O-TTPS Description
PR.AC-1: Identities and credentials are managed for authorized devices and users.
4.2.1.3 SC_ACC: Access Controls
Proper access controls are established for the protection of product-relevant intellectual property against the introduction of tainted and counterfeit components where applicable in the supply chain. Access controls can vary by type of intellectual property and over time, during the life cycle.

Table 3: Framework Core

• PR.AC-3

NIST CSF Subcategory
O-TTPS Attribute/ Requirement
O-TTPS Description
PR.AC-3: Remote access is managed.
4.1.1.5 PD_PSM.03: Product Sustainment Management
Release maintenance shall include a product update process, which uses security mechanisms.

Table 3: Framework Core

• PR.DS-2

NIST CSF Subcategory
O-TTPS Attribute/ Requirement
O-TTPS Description
PR.DS-2: Data-in-transit is protected.
4.2.1.9 SC_STH: Secure Transmission and Handling
Secure transmission and handling of assets and artifacts during delivery is needed to lower the risk of product tampering while in transit to their destination.

Table 3: Framework Core

• PR.DS-3

NIST CSF Subcategory
O-TTPS Attribute/ Requirement
O-TTPS Description
PR.DS-3: Assets are formally managed throughout removal, transfer, and disposition.
4.2.1.11 SC_CTM: Counterfeit Mitigation
Practices are deployed to manufacture, deliver, and service products that do not contain counterfeit components.
Practices are deployed to control the unauthorized use of scrap from the hardware manufacturing process.

Table 3: Framework Core

• PR.DS-6

NIST CSF Subcategory
O-TTPS Attribute/ Requirement
O-TTPS Description
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information.
4.2.1.9 SC_STH.07: Secure Transmission and Handling
Methods of verifying authenticity and integrity of products after delivery should be available

Table 3: Framework Core

• PR.DS-8

• OTTPS (ISO/IEC 20243) SC_STH.07 e.g. verifying authenticity and integrity of products after delivery should be available

Table 3: Framework Core

• PR.MA-1

NIST CSF Subcategory
O-TTPS Attribute/ Requirement
O-TTPS Description
PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools.
4.1.1.5 PD_PSM.03: Product Sustainment Management
Release maintenance shall include a product update process, which uses security mechanisms.

Table 3: Framework Core

• DE.CM-4

NIST CSF Subcategory
O-TTPS Attribute/ Requirement
O-TTPS Description
DE.CM-4: Malicious code is detected.
4.2.1.12 SC_MAL: Malware Detection
Practices are employed that mitigate as much as practical the inclusion of malware in components received from suppliers and components or products delivered to customers or integrators.

Table 3: Framework Core

• DE.CM-6

NIST CSF Subcategory
O-TTPS Attribute/ Requirement
O-TTPS Description
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.
4.1.2.3 SE_VAR.03: Vulnerability Analysis and Response
A process shall exist for governing notification of newly discovered and exploitable product vulnerabilities.
4.1.1.5 PD_PSM.02: Product Sustainment Management
Release maintenance shall include a process for notification to acquirers of product updates.

Table 3: Framework Core

• DE.CM-8

NIST CSF Subcategory
O-TTPS Attribute/ Requirement
O-TTPS Description
DE.CM-8: Vulnerability scans are performed.
4.1.2.3 SE_VAR.03: Vulnerability Analysis and Response
A process shall exist for governing notification of newly discovered and exploitable product vulnerabilities.
4.1.2.4 SE_PPR.02: Product Patching and Remediation
There should be a process for informing an acquirer of notification and remediation mechanisms.

Table 3: Framework Core

• Line 913

• Include Open Group's OTTPS (ISO/IEC 20243) as reference

Appendix B: Glossary

• “Critical Infrastructure”
• Will DHS update critical infrastructure to explicitly include protection of US voting infrastructure

[End Sticky Notes]

Dan Reddy