

<b>As of:</b> 4/25/22 12:45 PM
<b>Received:</b> April 22, 2022
<b>Status:</b> Pending_Post
<b>Tracking No.</b> 12a-vllq-ou35
<b>Comments Due:</b> April 25, 2022
<b>Submission Type:</b> Web

# PUBLIC SUBMISSION

**Docket:** NIST-2022-0001

Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

**Comment On:** NIST-2022-0001-0001  
RFI-2022-03642

**Document:** NIST-2022-0001-DRAFT-0032  
Comment on FR Doc # N/A

---

## Submitter Information

**Email:** [REDACTED]  
**Organization:** Professional Services Council

---

## General Comment

On behalf of the 400+ member companies of the Professional Services Council (PSC), I am pleased to submit comments on the National Institute of Standards and Technology's (NIST's) request for information (RFI) on "Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management" as published in the Federal Register on February 22, 2022.

NIST seeks through this RFI information to help in "evaluating and improving its cybersecurity resources, including the 'Framework for Improving Critical Infrastructure Cybersecurity' (the 'NIST Cybersecurity Framework,' 'CSF' or 'Framework') and a variety of existing and potential standards, guidelines, and other information, including those relating to improving cybersecurity in supply chains. NIST is considering updating the NIST Cybersecurity Framework to account for the changing landscape of cybersecurity risks, technologies, and resources." With these NIST goals in mind, PSC solicited feedback from the government technology and professional services companies that make up its membership—companies whose support to federal agencies includes, but is not limited to, information technology, engineering, logistics, facilities management, consulting, international development, and scientific, social, and services.

The detailed observations and recommendations below align with the topics listed in the RFI under (1) Use of the NIST Cybersecurity Framework, (2) Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources, and (3) Cybersecurity Supply Chain Risk Management. In general, though, it is worth noting that PSC considers this request for information as a useful jumping-off point for continued, robust dialogue between industry and NIST on cybersecurity standards and recommends successive engagements involving the relevant trade associations, their member companies, and NIST in advance of rulemaking on this issue set.

Please see attached PDF for detailed comments and recommendations. Thank you for your consideration.

---

# Attachments

PSC Comments on NIST Cybersecurity RFI

April 22, 2022

National Institute of Standards and Technology  
ATTN: Katherine MacFarland  
100 Bureau Drive, Stop 2000  
Gaithersburg, MD 20899

**RE: PSC Comments on NIST Request for Information on “Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management” [Docket Number 220210-0045]**

Dear Ms. MacFarland:

On behalf of the 400+ member companies of the Professional Services Council (PSC),<sup>1</sup> I am pleased to submit comments on the National Institute of Standards and Technology’s (NIST’s) request for information (RFI) on “Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management” as published in the Federal Register on February 22, 2022.

NIST seeks through this RFI information to help in “evaluating and improving its cybersecurity resources, including the ‘Framework for Improving Critical Infrastructure Cybersecurity’ (the ‘NIST Cybersecurity Framework,’ ‘CSF’ or ‘Framework’) and a variety of existing and potential standards, guidelines, and other information, including those relating to improving cybersecurity in supply chains. NIST is considering updating the NIST Cybersecurity Framework to account for the changing landscape of cybersecurity risks, technologies, and resources.”<sup>2</sup> With these NIST goals in mind, PSC solicited feedback from the government technology and professional services companies that make up its membership—companies whose support to federal agencies includes, but is not limited to, information technology, engineering, logistics, facilities management, consulting, international development, and scientific, social, and environmental services.

The detailed observations and recommendations below align with the topics listed in the RFI under **(1) Use of the NIST Cybersecurity Framework, (2) Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources, and (3) Cybersecurity Supply Chain Risk Management**. In general, though, it is worth noting that **PSC considers this request for information as a useful jumping-off point for continued, robust dialogue between industry and NIST on cybersecurity standards and recommends successive engagements involving the relevant trade associations, their member companies, and NIST in advance of rulemaking on this issue set.**

---

<sup>1</sup> PSC is the voice of the government technology and professional services industry, representing the full range and diversity of the information technology and professional services sector that supports U.S. federal missions. Our 400+ members include small, medium, and large businesses that specialize in services, including but not limited to information technology, engineering, logistics, facilities management, consulting, international development, scientific, social, environmental services, and more. Together, the association’s members employ hundreds of thousands of Americans in all 50 states.

<sup>2</sup> “[Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management](#); notice; request for information,” 87 Federal Register 35 (22 Feb 2022), pp. 9579-9581

**Topic (1): Use of the NIST Cybersecurity Framework**

1. *The usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions in the Framework and actively managing risks using those five functions.*

PSC believes the CSF aids companies in organizing cybersecurity efforts. Specifically, its usefulness derives from its ability to provide an approachable framework to organize cybersecurity activities, help facilitate communication regarding risk and how risk is considered within the organization, and prioritize opportunities aligned with objectives and requirements. The CSF supports organizations in integrating key functions into their security approaches.

Specifically regarding NIST’s published Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Guidance, one PSC member notes that its work to integrate SCRM Guidance into its approach to customer solutions includes mapping the SCRM program. This approach builds out a “Supply Chain Security Operations Center” (SOC) concept, which operates in concert with the Cyber SOC and increases operational efficiencies through symmetric security and incident response processes. Challenges or inefficiencies in integration have led to the following comments/recommendations:

- **SCRM High-Level Alignment with the CSF:** The *NIST Special Publication (SP) 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations* framework is built on four functions: “Frame, Assess, Respond and Monitor.” (see *Figure 1*). Aligning the different framework requires (at times, significant) effort that can require the development of a translation document, which must be updated regularly to maintain currency.

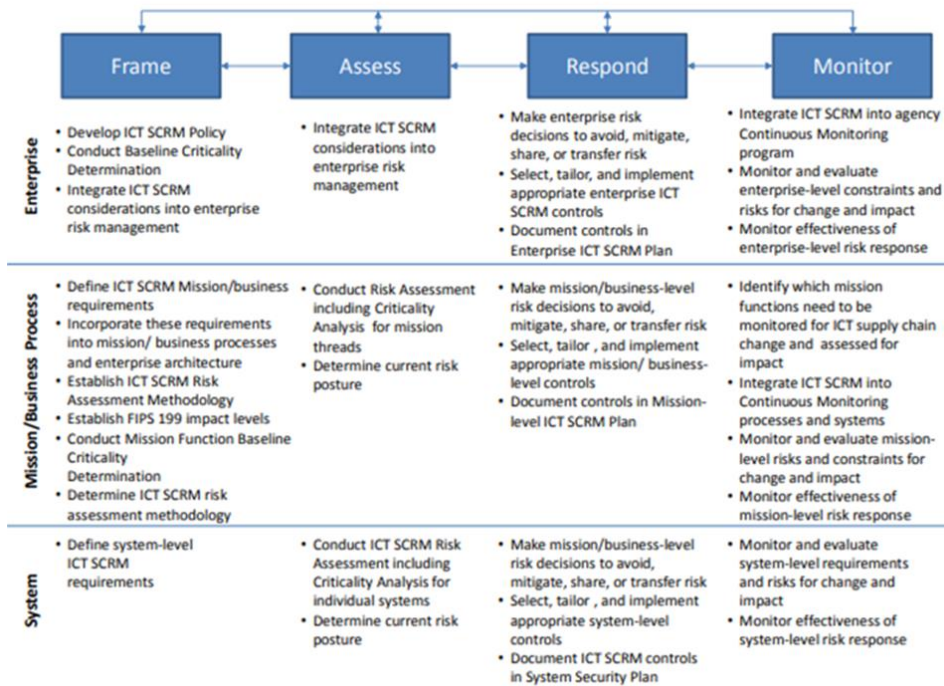


Figure 1: ICT SCRM Framework from Figure 2-4 of NIST SP 800-161

**Recommendation: Consider adjusting NIST 800-161’s approach to map to the CSF five functions more explicitly.** This will increase the ease of adoption across industry and deliver more successful implementations of cohesive and integrated security programs.

- **Alignment of SCRM Categories within CSF:** The CSF Core specifically addresses SCRM within the “Identify” function as the category Supply Chain Risk Management (ID.SC), with subcategories ID.SC-1 through ID.SC-5. Some of these subcategories, however, appear to be more appropriately mapped to other functions within the CSF Core, or otherwise worthy of amplification within the text of the Core:
  - **ID.SC-3:** ID.SC-3 states “Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan.”<sup>3</sup> There is a component here that is appropriate for the “Identify” function, in that the implementer should identify the appropriate contractual requirements to invoke upon suppliers. These requirements may include (1) appropriate evidence and/or attestations of secure software development practices; (2) requirements for notifications regarding foreign ownership, control, or influence (FOCI) changes; (3) software bill of materials (SBOMs); and (4) vulnerability disclosure program (VDP) participation as appropriate.

**These requirements, however, do not have a corresponding subcategory in the “Detect” function, and the operationalization of these contract requirements should be reflected in other areas within the framework, similar to other cyber operations.** As an example, integrating SBOMs into vulnerability management programs and consuming vulnerability exchange (VEX) data to detect for issues, or monitoring upstream suppliers for risk indicators such as breaches, financial stress, FOCI changes, etc. would be appropriate for reference in the “Detect” function as dedicated subcategories akin to continuous monitoring. Further, as any anomalies triggered by supply chain oversight should be formally responded to, adding an appropriate subcategory to the “Respond” function would be useful. **Additionally, in the “Informative References” table for ID.SC-3, a direct reference to NIST SP 800-161 might be beneficial.**

- **ID.SC-4:** ID.SC-4 states “Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.”<sup>4</sup> **Similar to the rationale above, this appears to be an operational action that is better suited to the “Detect” function.**
- **ID.SC-5:** ID.SC-5 states “Response and recovery planning and testing are conducted with suppliers and third-party providers.”<sup>5</sup> This critical function parallels that in Information Protection Processes and Procedures (PR.IP) subcategory 10 (PR.IP-10), which states that “Response and recovery plans are tested.”<sup>6</sup> **Similarly, it would be**

---

<sup>3</sup> <https://csf.tools/reference/nist-cybersecurity-framework/v1-1/id/id-sc/id-sc-3/>

<sup>4</sup> <https://csf.tools/reference/nist-cybersecurity-framework/v1-1/id/id-sc/id-sc-4/>

<sup>5</sup> <https://csf.tools/reference/nist-cybersecurity-framework/v1-1/id/id-sc/id-sc-5/>

<sup>6</sup> <https://csf.tools/reference/nist-cybersecurity-framework/v1-1/pr/pr-ip/pr-ip-10/>

**appropriate for ID.SC-5 to be merged with (by explicit expansion) PR.IP-10 or given its own place within the “Protect” function for exercising such plans.**

*2. Current benefits of using the NIST Cybersecurity Framework. Are communications improved within and between organizations and entities (e.g., supply chain partners, customers, or insurers)? Does the Framework allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks? What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?*

For current benefits, one PSC member measures itself against the maturity of the CSF subcategories and averages the aggregate scores to the category and functions levels. They are thus able to evaluate and compare their maturity to other industry stakeholders. **While this might improve upon cyber assessments and comparing assessments between organizations, relevant metrics for improvement would be a change to the maturity levels definitions.** For example, some entities use maturity scores that are aligned with the Software Engineering Capability Maturity Model (SEI-CMM) levels rather than NIST CSF maturity scores. PSC members have found that peer companies in specific sectors use nearly the same SEC-CMM - based definitions for their maturity levels, and the NIST maturity level definitions are not as common or well known within the industry.

For contractors, each agency can require different performance execution and utilization of NIST standards. **To make metrics more relevant and analogous to work required, it is essential that metrics are defined by a family of requirements and security/cyber controls, as well as the total infrastructure.** For example, focusing on software development and then installing it without considering the hardware standards for cyber safety still allows room for cyber risk.

The Cybersecurity Framework extensively references NIST SP 800-53 Revision 4 with regard to supply chain integrity controls and standards. The NIST SP 800-161 also has an extensive set of controls and processes for implementation of supply chain security and ensuring supply chain integrity. NIST SP 800-161 also references NIST SP 800-53 Revision 4 throughout, causing some confusing loops when trying to plot a course for supply chain integrity approaches—this is one example of a pattern recognized across multiple special publications produced by NIST.

To interpret, implement, document, and validate the framework, a business is required to employ at least five different resources with individual skillsets. The alternative practice of hiring consulting firms creates a difficult barrier to entry for many small businesses. While these barriers help ensure that cybersecurity is properly addressed in government systems, they can often prevent innovative and effective solutions from making it to market.

- **Recommendation: Develop a set of targeted “playbooks” that provide specific approaches based on qualifying factors.** A simple example would be to target a general industry such as software development and provide guiding examples to implement cybersecurity controls into the application lifecycle. IT consultants could use a playbook targeting common systems they support, such as domain management and email hosting solutions. All of these playbooks should follow best practices, such as zero trust architecture. These playbooks could reduce time to entry by giving technologists the ability to implement with security already "baked in."

3. *Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively (e.g., resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity).*

- **Organizational factors:** NIST developed the CSF to be flexibly applied to organizations, which can also result in varying interpretations in some areas. For example, organizations could spend significant time and resources to understand and apply certain subcategories of the CSF.
- **Resource issues:** Vendors, especially small businesses, could face challenges in implementing the CSF if they do not have a dedicated cybersecurity and/or IT support team. Suppliers typically apply higher-level security controls based on the product or service provided, or they rely on a third-party provider's interpretation of required controls.
- **Information-sharing:** While NIST provides information references, they vary in terms of clarity and usefulness. For example, a PSC member is still assessing how to apply ID.BE-1 and ID.BE-2 in assigning ownership and rating maturity.
- **Knowledge levels and experience considerations:** Gaps in knowledgeable workforce and familiarity with NIST CSF. While the NIST website provides several case studies, it may be difficult to apply these to a specific organization.
- **Agency factors:** Competing agency compliance priorities can complicate companies' calculations and approach to an opportunity.

Like DoD's Cybersecurity Maturity Model Certification, the CSF is primarily a U.S.-centric framework. Given that international suppliers follow cybersecurity requirements of their respective governments, there is the potential for complex—if not contradictory—guidance in the global supply chain.

4. *Any features of the NIST Cybersecurity Framework that should be changed, added, or removed. These might include additions or modifications of: Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines; guidance on how to use the Cybersecurity Framework; or references to critical infrastructure versus the Framework's broader use.*

This topic leads to several **observations/recommendations**:

- **Make PR.AC-1 a category of its own and reduce unnecessarily duplication/redundancy elsewhere, especially related to seemingly redundant detecting and incident response subcategories.** Under PR.AC-1, identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes. Unlike RC.CO-1 and RC.CO-2, this is a very large subcategory, and it can be difficult to rate companies effectively.

- **Generally, the subcategory’s “intent” should be more explicit**, so they are less subject to interpretation across industry. In addition, “intent” should translate into “what is the overall need for the subcategory or how does it apply.”
- **As the present CSF names the subcategory and informative references, include a few sentences that describe the purpose of the subcategory.** For example, in the ID.AM-2: Software platforms and applications within the organization are inventoried subcategory, the CSF could clarify that this is for software, applications, and operating systems (if that is the intent). To maintain the flexibility, the description could start with “Generally this subcategory means”.
- **Make changes incrementally and not at such a level that it would cause major updates to an organization’s process.**
- **The addition of NIST SP 800-171 to informative references would provide value to defense industrial base companies that must implement NIST SP 800-171 as a result of defense contracts.**
- **Define what is considered “critical infrastructure” – perhaps through a list by user community.** There is not a standard critical infrastructure definition that is being universally communicated.

*5. Impact to the usability and backward compatibility of the NIST Cybersecurity Framework if the structure of the framework such as Functions, Categories, Subcategories, etc. is modified or changed.*

- **Recommendation: Conduct a gap analysis to help set a new target profile incorporating modifications or changes.** While impacts are low to moderate, depending on the level of change, changes will impact companies differently.

*6. Additional ways in which NIST could improve the Cybersecurity Framework or make it more useful.*

- **Recommendations:**
  - **Provide clearer guidance on how companies should put together framework profiles using a standardized approach.** While NIST provided a Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide, industry believes this example too complex.
  - **Recommendation: Provide guidance on preparing profiles in a standardized way tailored to industry and by sector.** Additional guidance is also needed when it comes to using the same controls in different areas and not creating multiple profiles in the same company.



## **Topic (2): Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources**

7. *Suggestions for improving alignment or integration of the Cybersecurity Framework with other NIST risk management resources. As part of the response, please indicate benefits and challenges of using these resources alone or in conjunction with the Cybersecurity Framework.*

- *Risk management resources such as the NIST Risk Management Framework, the NIST Privacy Framework, and Integrating Cybersecurity and Enterprise Risk Management (NISTIR 8286). **Recommendation: Harmonize NIST standards/resources across the federal government.***
- *Trustworthy technology resources such as the NIST Secure Software Development Framework, the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline, and the Guide to Industrial Control System Cybersecurity. **Recommendation: Incorporate NIST documents/resources into one supporting document that can be cross-referenced to the applicable family/control.***
- *Workforce management resources such as the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity. One PSC member has leveraged the NICE Framework for building models of cybersecurity organization implementations. As this framework requires extension to align insider threat SOC functions with the cyber SOC functions, this member sees a similar need for extension regarding SCRM integration within a SOC construct. **Recommendations: The Securely Provision – Risk Management section of the framework should include roles, tasks, and knowledge-skills-abilities (KSAs) for SCRM analysts as well. This extension will aid in aligning and utilizing the NICE Framework with the CSF, as they are quite complimentary. Educational training modules with proof of certification for industry could also prove beneficial.***

8. *Use of non-NIST frameworks or approaches in conjunction with the NIST Cybersecurity Framework: Are there commonalities or conflicts between the NIST framework and other voluntary, consensus resources? Are there commonalities or conflicts between the NIST framework and cybersecurity-related mandates or resources from government agencies? Are there ways to improve alignment or integration of the NIST framework with other frameworks, such as international approaches like the ISO/IEC 27000-series, including ISO/IEC TS 27110?*

- *Supplier of all sizes will have security principles of all sizes. Having the ability to connect like or related elements would help increase the fidelity of risk determination and reduce workload. **Recommendation: Robust alignment or capability/capacity to connect like items would be a benefit when working with the supply chain.***
- *The ISO-based security is very common in the non-government technology and commercial areas, especially outside of the United States where NIST is considered U.S. only. **Recommendation: Increase alignment between the CSF and the ISO/IEC 27000-series.***

- NIST is driving quality to their own standards of cyber performance. ISO certifications need to consider NIST Cybersecurity Framework impacts to guarantee there is no conflict in directions being given to both government and industry. **Recommendation: Align ISO and NIST.**

9. *There are numerous examples of international adaptations of the Cybersecurity Framework by other countries. The continued use of international standards for cybersecurity, with a focus on interoperability, security, usability, and resilience can promote innovation and competitiveness while enabling organizations to more easily and effectively integrate new technologies and services. Given this importance, what steps should NIST consider to ensure any update increases international use of the Cybersecurity Framework?*

- **Recommendations:**
  - **Step 1: NIST should maintain a good mapping to the main international standards, such as the ISO/IEC 27000-series.**
  - **Step 2: NIST should develop a dedicated international board that includes hardware, software, and Cloud/ICT certification standards to drive universal adaption of NIST methodologies.**

10. *References that should be considered for inclusion within NIST's Online Informative References Program. This program is an effort to define standardized relationships between NIST and industry resources and elements of documents, products, and services and various NIST documents such as the NIST Cybersecurity Framework, NIST Privacy Framework, Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53), NIST Secure Software Development Framework, and the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline.*

Regarding references for inclusion within NIST's Online Informative References Program, **PSC suggests that NIST must decide what reference is the authoritative, or top-down reference, that influences other external standards, documents, policies, etc.** Contracting Officers must clearly define within the request for proposal the dependency and future performance requirements that need to be solutioned. Requests for proposals should also identify and, if needed, define what NIST standards are being evaluated for the award selection process.

### **Topic (3): Cybersecurity Supply Chain Risk Management**

11. *National Initiative for Improving Cybersecurity in Supply Chains (NIICS): What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address? How can NIST build on its current work on supply chain security, including software security work stemming from E.O. 14028, to increase trust and assurance in technology products, devices, and services?*

- **Recommendation: NIICS should address resourcing and/or financial issues that small and medium-sized suppliers face regarding how to obtain/acquire and implement**

**cybersecurity services**—particularly companies that do not have dedicated cybersecurity/IT teams or the infrastructure to implement needed changes to compete for contracts. For these companies, the cost of executing robust cyber defenses is often significantly larger than the cost of the product or service they are providing.

- **Recommendation: Defining “Cyber Security Supply Chain Risk.”** There are multiple NIST standards, references, and definitions that continue to cause confusion. Each definition is mapped from a different document of record.

Overall, the current NIST Cybersecurity Framework Supply Chain Risk Management focuses on advanced planning processes (e.g., supply chain risk assessment, supplier contracts, supplier assessments and recovery plans). Planning should be a continuous process, managing change to increase flexibility through new models, such as Supply Chain as a Service and systems that provide real-time, end-to-end transparency of software suppliers and the provenance of commercial and open-source software.

*12. Approaches, tools, standards, guidelines, or other resources necessary for managing cybersecurity-related risks in supply chains. NIST welcomes input on such resources in narrowly defined areas (e.g. pieces of hardware or software assurance or assured services, or specific to only one or two sectors) that may be useful to utilize more broadly; potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, or stakeholders; as well as large-scale and extremely difficult areas.*

While the CSF is not intended to be a standalone, all-inclusive compendium of information, it does provide information on communicating cybersecurity requirements, including those pertaining to SCRM. Considerations should include discussion on relevant fundamental elements of the Secure Software Development Framework and other pertinent definitions and references for “critical software,” SBOM, and Supplier Declaration of Conformance, as they have clear and distinct impacts to supply chain requirements and overall cybersecurity.

- **Recommendations: Delineate roles and responsibilities of government, consumer, prime and subcontractor, industry provider, and manufacturer throughout the acquisition lifecycle process. Leverage advanced analytics to continuously assess cyber risk trends related to supplier software assurance and assured services.**

*13. Are there gaps observed in existing cybersecurity supply chain risk management guidance and resources, including how they apply to information and communications technology, operational technology, IoT, and industrial IoT? In addition, do NIST software and supply chain guidance and resources appropriately address cybersecurity challenges associated with open-source software? Are there additional approaches, tools, standards, guidelines, or other resources that NIST should consider to achieve greater assurance throughout the software supply chain, including for open-source software?*

- **Recommendation: Regarding open-source, NIST should consider developing a standard for developing and registering an approved list of open-source software/materials.** There has been an increase in software supply chain attacks that exploit upstream open source ecosystems.

- **Recommendation: The NIST software supply chain guidance and resources need increased emphasis on dependency management by software development teams with guidance on methods to assess and manage security risks and identify dependencies that are stale or susceptible to increased security risks.**
- **Recommendation: Provide guidance on how to deploy intelligent automation and analysis systems.**

*14. Integration of Framework and Cybersecurity Supply Chain Risk Management Guidance. Whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated NIST Cybersecurity Framework—or whether and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately be developed by NIST.*

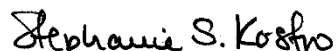
If any new and separate NIST Cybersecurity Framework is created, NIST must map all levels of tiered architecture dependencies throughout the acquisition lifecycle. NIST and the Cybersecurity and Infrastructure Security Agency must collaborate to pull together the "cyber risk" of an ICT product compared to an ICT service that can create the risk.

---

PSC appreciates NIST's willingness to engage with industry on a range of issues that are important to our nation's security and economic well-being. This engagement, of course, is an iterative process, and it could only benefit from more forums for open dialogue and discussion. As an industry association representing these businesses, we at PSC look forward to continued engagement and would be happy to facilitate such interactions, as appropriate.

Should you have any questions, please feel free to contact me at [REDACTED]. Thank you for your consideration.

Sincerely,



Stephanie S. Kostro  
Executive Vice President for Policy