PSC PROFESSIONAL SERVICES COUNCIL

March 16, 2023

Ms. Cherilyn Pascoe
Senior Technology Policy Advisor and
NIST Cybersecurity Framework Program Lead
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

RE: PSC Comments on NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework

Dear Ms. Pascoe:

On behalf of the 400-plus member companies of the Professional Services Council (PSC),[1] I am pleased to submit comments on the National Institute of Standards and Technology's (NIST's) ***Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework*** (Concept Paper), published on the NIST Computer Security Resource Center's webpage on January 19, 2023. By releasing this Concept Paper for public comment, NIST has again demonstrated its commitment to seeking additional input on the structure and direction of the Cybersecurity Framework, and as noted in the Concept Paper, NIST is considering significant changes in CSF 2.0,[2] many of which are important to the government contracting industry that supports federal missions.

PSC appreciates that the Concept Paper reflects industry feedback on NIST's February 2022 **request for information (RFI),** *Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management*. PSC's **response to that RFI** highlighted how the notice served "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."[3] **PSC recognizes that NIST officials continue to pursue meaningful industry engagement on the Cybersecurity Framework and to incorporate feedback, as appropriate, on CSF 2.0.** With that in mind, PSC's comments and recommendations below align with the six categories of "potential significant changes in CSF 2.0" as outlined in the Concept Paper. Please note that PSC's recommendations are both **bolded and underlined**.

[1] PSC is a trade association representing the government technology and professional services industry. PSC's 440+ member companies are small, medium, and large businesses that provide federal agencies with essential services including, but not limited to, information technology, engineering, logistics, facilities management, sustainment, consulting, international development, and scientific, social, and environmental services. These companies represent the full range and diversity of the government services sector.

[2] NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework. (2023, January 19). National Institute of Standards and Technology. Retrieved from https://csrc nist.gov/News/2023/csf-2-0-concept-paper-released

[3] 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]. (2022, April 22). PSC. Retrieved from https://www.pscouncil.org/a/Resources/2022/PSC_NISTRFI_Comments_20220422.aspx?WebsiteKey=502af8cb-491d-4e9b-b350-c7e3ff5bb9ee

Category 1: CSF 2.0 will explicitly recognize the CSF's broad use to clarify its potential applications

1.1. Change the CSF's title and text to reflect its intended use by all organizations

PSC recognizes both NIST's rationale for changing the framework's title from "Framework for Improving Critical Infrastructure Cybersecurity" to "Cybersecurity Framework" and the fact that companies in our nation's diverse industrial base will reflect CSF guidance according to their size, cyber infrastructure, needs, and potential risks. Though this title change in and of itself may not necessarily alter how those companies address cybersecurity risks, the mindset behind how stakeholders apply the CSF to their organizations could change if CSF language is applied more broadly.

Broadening the CSF's title and scope may improve the usability and accessibility for various organizations, but at least two suggestions may help mitigate potential confusion. **NIST should better define "critical infrastructure" for different types of organizations; clarity will help companies to apply CSF 2.0 more effectively. NIST should also consider developing and promulgating guides, graphics, and simplified guidance documents that can be visually referenced by non-technical audiences.**

1.2. Scope the CSF to ensure it benefits organizations regardless of sector, type, or size

As cybersecurity risk affects a diversity of organizations, NIST should apply the CSF more broadly so different types of organizations—e.g., academia, government agencies, industry—can implement guidance to protect their infrastructure. Each organization, of course, will need to implement guidance in a fashion tailored to its individual needs.

In PSC's April 2022 comments referenced above, member companies provided insight into key areas related to the broad applicability of the CSF:

- **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.

  NIST should explicitly state how different organizations should use CSF guidance (i.e., map out how organizations should implement the CSF by sector, type, or size in order to avoid confusion).

- **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.

  NIST should provide guidance on preparing profiles in a standardized way, based on industry and sector. Additional guidance is also needed regarding using the same controls in different areas and avoiding unnecessary duplication of profiles within the same company.

1.3. Increase international collaboration and engagement

Overall, PSC believes making the CSF broader and more internationally collaborative parallels the erosion of barriers in the digital space regarding both international regulations and adversarial tools, tactics, and procedures.

Category 2: CSF 2.0 will remain a framework, providing context and connections to existing standards and resources

2.1. Retain CSF's current level of detail

Generally, PSC believe the CSF's flexibility and level of detail are among its main benefits. So long as those characteristics are not compromised, improvements will likely be proactive and productive regarding adoption and implementation.

2.2. Relate the CSF clearly to other NIST frameworks

Regarding other NIST frameworks, the Concept Paper states, "Each focuses on specific topics worthy of dedicated guidance. However, as commenters pointed out, each framework has a relationship with the CSF, so they will be referenced as guidance either in CSF 2.0 or in companion materials, such as mappings."[4] A PSC member company official noted that the CSF already catalogues and organizes multiple cybersecurity standards, best practices, checklists, and frameworks. A structure that further highlights the crossover and conflicts between different rulesets could improve adoption.

Section 2.4. partially addresses this concern. A dynamic mapping—that can be more easily managed than edition-based releases—might prove useful. **NIST should explain to stakeholders how it plans to incorporate or reference updated / revised / newly published NIST frameworks within CSF 2.0.** Will NIST revise CSF as new NIST frameworks emerge? If so, how will NIST solicit public feedback?

Regarding structure, PSC's April 2022 comments highlighted several recommendations that could support such companion materials, such as mappings:

- 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.

[4] NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework. (2023, January 19). National Institute of Standards and Technology. Retrieved from https://csrc nist.gov/News/2023/csf-2-0-concept-paper-released

- 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 **<u>one</u>** supporting document that can be cross-referenced to the applicable family/control.

2.2. and 2.3. Leverage Cybersecurity and Privacy Reference Tool for online CSF 2.0 Core

A PSC member company official noted that it may be beneficial to incorporate additional privacy best practices and regulatory frameworks and upcoming CMMC 2.0 requirements. **This member observed that Sections 2.2. and 2.3. underscore that CSF 2.0 will reference privacy and other frameworks; reducing the conflict between privacy and security could be given higher priority.**

Category 3: CSF 2.0 (and companion resources) will include updated and expanded guidance on Framework implementation

3.1. Add implementation examples for CSF Subcategories / 3.2. Develop a CSF Profile template

In support of the broadened CSF, **<u>NIST should consider developing and promulgating sector, stakeholder, or size-specific versions or quick-start reference guides.</u>** Section 3.1. and 3.2. indicate this may be the direction the CSF 2.0 will take, but different sub-versions for specific sectors or stakeholder sizes would greatly improve accessibility.

Category 4: CSF 2.0 will emphasize the importance of cybersecurity governance

Overall, **<u>PSC believes defining roles, responsibilities, and proactive action according to a stakeholder approach would be beneficial.</u>** Such clarity can support implementation, even as NIST strives to broaden the framework.

4.1. Add a new Govern Function / 4.2. Improve discussion of relationship to risk management

PSC welcomes the addition of a new Govern function within the Cybersecurity Framework. Cybersecurity within an organization does not occur in a vacuum and must resonate strongly with that organization’s governance structure and the officials who provide guidance to the organization as a whole – meaning, top leaders must buy into the need for cybersecurity, the organization’s cybersecurity plan, and the risk management that accompanies it. Moreover, appropriate governance will connect cybersecurity to other key functions within an organization, making cyber activity (identify, detect, protect, respond) ubiquitous and second nature across the enterprise.

Therefore, PSC appreciates that the Concept Paper sections 4.1. and 4.2. address improved governance and risk management language. **Clarifying the need to define the roles and responsibilities within supply chain stakeholders, contractors, services, etc. would also improve clarity and outcomes around risk management discussions.**

Category 5: CSF 2.0 will emphasize the importance of cybersecurity supply chain risk management (C-SCRM)

5.1. Expand coverage of supply chain

PSC's April 2022 comments provided NIST with PSC member input regarding C-SCRM; the message was that there must be alignment between C-SCRM and any draft CSF 2.0. Those comments also specifically outlined several recommendations that NIST has listed as options in its CSF 2.0 Concept Paper, including:

- Further integrating C-SCRM outcomes throughout the CSF Core across Functions (integration may include supply chain separately or as a consideration as part of broader outcomes)

  PSC Comment: 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.

- Expanding C-SCRM outcomes within the current ID.SC Category in the Identify Function

  PSC Comment: While the CSF Core specifically addresses C-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.

  For example, other functions such as "Detect" or "Protect" may be better suited for operational action than the "Identify" function.

On a related note, PSC and its member companies understand that NIST officials have expressed interest in understanding whether Supply Chain issues may be addressed separately within CSF 2.0 or as part of an existing function. PSC understands the need to highlight the importance of Supply Chain elements within any Cybersecurity Framework and considers SCRM an integral thread woven throughout the entirety of the framework. The concern regarding moving Supply Chain into a separate (sixth) CSF function is that such separation may dilute the SCRM-related roles and responsibilities that are most appropriately addressed as categories or sub-categories of those other functions. By moving Supply Chain activities to a separate (sixth) function ignores the fact that to be effective, SCRM must be ubiquitous throughout an organization's holistic approach to cybersecurity.

Therefore, **PSC encourages NIST to consider making "direct development of, approve, and maintain oversight over a Supply Chain Risk Management plan" a required element within the Govern function and to include SCRM responsibilities throughout each of the remaining four functions.** Such treatment could allow NIST to weave into those functions the supply-chain elements, such as cyber insurance and incident response, that are most relevant to each of them.

Category 6: CSF 2.0 will advance understanding of cybersecurity measurement and assessment

6.1. Clarify how leveraging the CSF can support the measurement and assessment of cybersecurity programs / 6.2. Provide examples of measurement and assessment using the CSF / 6.3. Update the NIST Performance Measurement Guide for Information Security

PSC notes that within these sections, the Concept Paper suggests that CSF 2.0 will improve the language concerning risk measurement and assessment. Offering methodologies that are both quantitative and qualitative would help reach different audiences.

NIST should provide greater focus on quantifying risk according to financial business outcomes that can more effectively be communicated to C-suite level decision-makers.

PSC appreciates NIST's ongoing engagement with industry on CSF 2.0 and looks forward to a draft CSF 2.0 later this summer. 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 companies that provide critical technology and professional services to the federal government, 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 [redacted] Thank you for your consideration.

Sincerely,

Stephanie S. Kostro

Stephanie S. Kostro
Executive Vice President for Policy