November 6, 2023

BY EMAIL

National Institute of Standards and Technology (NIST)
Information Technology Laboratory
Applied Cybersecurity Division
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899
cyberframework@nist.gov

Re: Draft NIST Cybersecurity Framework 2.0

To Whom It May Concern:

CTIA,[1] NTCA –The Rural Broadband Association ("NTCA"),[2] and the Professional Services Council ("PSC")[3] appreciate the opportunity for continued engagement with NIST as it moves forward with developing Version 2.0 of the Cybersecurity Framework ("CSF"). We have been pleased to submit feedback to NIST through the CSF 2.0 development process[4]—including most recently in response to

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] NTCA–The Rural Broadband Association represents approximately 850 independent, community-based companies and cooperatives that provide advanced communications services in rural America and more than 400 other firms that support or are themselves engaged in the provision of such services.

[3] 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.

[4] *See* Comments of CTIA, NIST Cybersecurity Framework 2.0: Discussion Draft of the NIST Cybersecurity Framework 2.0 Core (filed May 31, 2023), https://www.nist.gov/system/files/documents/2023/08/04/CTIA%20Comments%2005312023%20Discussion%20Draft_Redacted.pdf ("CTIA Draft 2.0 Core Comments"); Comments of NTCA, NIST Cybersecurity Framework 2.0 Concept Paper, (filed Mar. 17, 2023), https://www.nist.gov/system/files/documents/2023/04/26/2023-03-17%20NTCA_508_Redacted.pdf; Comments of PSC, Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management, Docket No. 220210-0045 (filed Apr. 22, 2022), https://www.nist.gov/system/files/documents/2023/04/26/2023-03-17%20PSC_508_redacted.pdf; Comments of CTIA, Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management, Docket No. 220210-0045, NIST (filed Apr. 25, 2022), https://www.nist.gov/system/files/documents/2022/05/03/04-25-2022%20-%20CTIA.pdf; Comments of NTCA, Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management, Docket No. 220210-0045, NIST (filed Apr. 25, 2022), https://www.nist.gov/system/files/documents/2022/05/03/04-25-2022%20-%20NTCA.pdf; Letter from Thomas K.

NIST's Discussion Draft of the CSF 2.0 Core ("Draft 2.0 Core").[5] We write this letter to reiterate a key theme from our past advocacy: in order to maximize the benefits of the update to the CSF 2.0 and limit negative impacts caused by unnecessary changes to the CSF, NIST should reject calls to create new Functions. In particular, with this letter, we urge NIST to reject calls to create a new seventh Function focused on cybersecurity supply chain risk management ("C-SCRM"), both to avoid significant backward compatibility issues and because the CSF already appropriately addresses complex and important C-SCRM issues.

The undersigned organizations agree that C-SCRM is critical to broader cyber efforts and urges NIST to stay the course with how it handles C-SCRM in the Draft CSF 2.0, which appropriately raises awareness of the importance of C-SCRM but does not try to address all of the complexities of C-SCRM within the CSF. As the undersigned noted in comments,[6] the treatment of C-SCRM in the Draft CSF 2.0—specifically, retaining a single C-SCRM Category and making modest updates to relevant Subcategories—is appropriate. As such, the undersigned organizations support the inclusion of C-SCRM guidance at the level of detail and organization that NIST has proposed in the Draft 2.0 Core and in the Draft CSF 2.0.[7] For example, CTIA, the wireless industry, and the Communications Sector agree that C-SCRM activities are of critical importance and have demonstrated a commitment to advancing C-SCRM, including by participating in the Department of Homeland Security's Information and Communications Technology Supply Chain Management Task Force,[8] and commenting on NIST's drafts of SP 800-161, Revision 1.[9]

A significant expansion of C-SCRM content in the CSF 2.0 would stretch the CSF beyond its intended scope and do a disservice to both the CSF and NIST's broader supply chain risk management ("SCRM") guidance. Providing C-SCRM guidance at the level sought by proponents of a new C-SCRM Function would undermine the framework approach and universal utility by focusing too closely on specific C-SCRM threats. Further, given the complexities of C-SCRM issues, NIST should continue the approach of providing insights and guidance through C-SCRM-specific workstreams, not the general CSF. In particular, the CSF is not the appropriate document to capture and contend with either the major

---

Sawanobori, Senior Vice President & Chief Technology Officer, CTIA to NIST (June 9, 2022) (regarding Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management).

[5] Discussion Draft of the NIST Cybersecurity Framework 2.0 Core, NIST (Apr. 24, 2023), https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf.

[6] CTIA Draft 2.0 Core Comments at 5-6; Comments of PSC, NIST Cybersecurity Framework 2.0: Concept Paper: Potential Significant Updates to the Cybersecurity Framework, NIST (filed Mar. 17, 2023), https://www.nist.gov/system/files/documents/2023/04/26/2023-03-17%20PSC_508_redacted.pdf.

[7] NIST Cybersecurity Framework 2.0, Initial Public Draft, (Aug. 8, 2023), NIST, https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd.

[8] *DHS and Private Sector Partners Establish Information and Communications Technology Supply Chain Risk Management Task Force*, CISA (Oct. 30, 2018), https://www.cisa.gov/news/2018/10/30/dhs-and-private-sector-partners-establish-information-and-communications-technology (last updated Feb. 5, 2021).

[9] *See, e.g.*, Comments of CTIA, Cyber Supply Chain Risk Management Practices for Systems and Organizations, NIST SP 800-161 (Rev. 1) (2nd Draft), NIST (filed Dec. 10, 2021).

differences in C-SCRM activities across sectors and types of companies and organizations, or the numerous other government C-SCRM guidance documents, which continue to evolve. Finally, SCRM risks and considerations extend well beyond cybersecurity, such as procurement, logistics, quality control, and privacy; the CSF is not the proper document to address these other considerations.

Creating a seventh C-SCRM Function would create more challenges than benefits. Adding a seventh function focused on C-SCRM guidance at this late stage in the CSF 2.0 development would cause confusion in the community, make the transition from CSF 1.1 to CSF 2.0 harder, and would inappropriately expand the scope and prescriptiveness of the CSF.

First, as a matter of process, NIST has properly and deliberately considered the issue of supply chain and third-party risk management, including in the CSF 2.0 Concept Paper[10] and public workshops and working sessions.[11] As noted above, in the face of some suggestions to add a supply chain Function, NIST did not include a seventh Function in the Draft CSF 2.0 Core or in the full Draft CSF 2.0. NIST has already completed a release and comment period on the Draft CSF 2.0 Core, and has now released the full CSF 2.0 Draft in August 2023 and asked for comments by November 4, so a fundamental change this late in the process would cause significant confusion across the community. NIST should not interpret silence from the community between the close of the comment period of the Draft CSF 2.0 Core and the release of the full Draft CSF 2.0 on the issue of a C-SCRM-focused function as acquiescence—rather, it likely reflects the widespread belief that adding further Functions was no longer open for consideration.

Second, adding a seventh Function would have significant "downstream" effects, for both organizations that have adopted the CSF and for the vast body of cybersecurity standards and guidance that use the CSF as a foundation. A wholesale change to the CSF's structure would force organizations that rely on the CSF to complete an additional set of mapping and reorganization activities to match the new structure. Products and services that use the CSF as an input or alignment structure, such as security management automation and cloud-based solutions, would have to be rebuilt. The wealth of federal government and private sector cybersecurity frameworks, profiles, other guidance, and standards that rely on or map to the CSF would have to be updated. International partners, too, such as Japan's Ministry of Economics, Trade, and Industry,[12] have built guidance tied to the CSF and would need to make further changes to adapt to a new C-SCRM Function. It is simply not worth the time and effort for organizations to do so when the proposed treatment of C-SCRM in the Draft CSF 2.0 is appropriate,

[10] NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework, NIST at 11-12 (Jan. 19, 2023), https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf.

[11] *Journey to the NIST Cybersecurity Framework (CSF) 2.0 | Workshop #2*, NIST, https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-workshop-2 (last updated Feb. 28, 2023); *Journey to the NIST Cybersecurity Framework (CSF) 2.0 | In-Person Working Sessions*, NIST, https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-person-working-sessions (last updated Feb. 16, 2023).

[12] The Cyber/Physical Security Framework, Version 1.0, Cyber Security Division, Commerce and Information Policy Bureau, Japan's Ministry of Economy, Trade and Industry ("METI") (Apr. 18, 2019), https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0_eng.pdf.

sufficient, and useful.

Third, in developing a seventh C-SCRM-focused Function, NIST might have to go beyond a simple remapping of existing Draft CSF 2.0 Categories and Subcategories—indeed, some of the previous proposals for a C-SCRM Function would create significant new and prescriptive content. Such an expansion would also likely result in the adoption of new terminology that would require additional community input and harmonization. The attached comparison chart identifies specific substantive differences between the Draft CSF 2.0 Categories and Subcategories, and one example proposal for a C-SCRM Function from another professional association. As noted in the chart, there are important unresolved questions about the scope of third party due diligence, whether and how to document a third party's cybersecurity practices as opposed the organization's own practices, and contractual provisions to effectuate an organization's C-SCRM policies and activities. Given the diversity among the types of organizations that rely on the CSF and the evolving best practices in the C-SCRM space, providing flexible and risk-based guidance on these specific areas in a more detailed manner as would be needed to justify a C-SCRM-specific Function would be extremely challenging at this time and would require significant further community input.

Given these substantive and procedural concerns, NIST should reject calls for a C-SCRM-specific Function and retain the proposed approach of maintaining C-SCRM as a Category, not a Function, in the CSF 2.0.

***

Each of our organizations has been proud to collaborate with NIST on the CSF since its introduction more than a decade ago. The CSF is a foundation for cybersecurity risk management efforts across the U.S. government and critical infrastructure, throughout the private sector, and around the world. NIST should therefore be extremely cautious in making fundamental changes to the CSF and should reject proposals to add a C-SCRM-specific Function.

Sincerely,

/s/ Thomas K. Sawanobori

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer
CTIA

/s/ Jill Canfield

Jill Canfield
General Counsel and VP of Policy
NTCA-The Rural Broadband Association

/s/Stephanie Kostro

Stephanie Kostro
Executive Vice President for Policy
PSC

Attachment

Comparison Between Financial Services Sector's Proposal for a C-SCRM Function ("Extend") and the Related Subcategories in Draft CSF 2.0

Category #1—Procurement Planning and Due Diligence (EX.DD): *Planning and due diligence are performed to reduce risks before entering into a formal third-party relationship*		
Proposed EX Subcategory Source: CRI Letter to NIST, 6/15/2023	**Closest Analogs in Draft CSF 2.0** Source: CSF 2.0 Draft, NIST,8/8/2023	**Substantive Differences**
EX.DD-01: Planning is performed for procurements and agreements that involve elevated risk to the organization	**GV.SC-07:** The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship. **GV.RR-04**: Roles and responsibilities for suppliers are established, documented in contractual language, and communicated	**EX.DD-01** appears to be less prescriptive and more general than the related Subcategories in Draft CSF 2.0. However, it refers to "planning" for third-party contracts, which is not specifically provided in Draft CSF 2.0.
EX.DD-02: The organization performs thorough due diligence on prospective third parties, consistent with procurement planning and commensurate with the level of risk, criticality, and complexity of each third-party relationship	**GV.SC-06**: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationship. **GV.SC-07**: The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship.	**EX.DD-02** is more prescriptive than the relevant Subcategories in Draft CSF 2.0, as it requires an organization to perform "*thorough* due diligence" on prospective third parties (emphasis added). It is also broader in scope, as applies to "prospective third parties."
EX.DD-03: The organization assesses the suitability of the technology and cybersecurity capabilities and risk management practices of prospective third parties	**GV.SC-07**: The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship **GV.SC-05**: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	**EX.DD-03** is broader in scope in that it applies to "prospective third parties," whereas the relevant Subcategories in Draft CSF 2.0 focus on current suppliers and third-party partners.
EX-DD-04: Third-party products and services are assessed relative to business, risk management, and cybersecurity requirements	**GV.SC-07**: The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	**EX-DD-04** extends beyond cybersecurity and requires assessments related to "business" and "risk management" requirements that are wholly separate from cybersecurity requirements

Category #2—Third-Party Contracts and Agreements (EX.CN): *Contracts establish baselines protections to manage risk over the life of the third-party relationship*		
Proposed EX Subcategory	**Closest Analogs in Draft CSF 2.0**	**Substantive Differences**
EX.CN-01: Contracts clearly specify the rights and responsibilities of each party and establish requirements to address the anticipated risks posed by a third party over the life of the relationship	**GV.SC-05**: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	**EX.CN-01** is more prescriptive (contracts must "*clearly* specify rights and responsibilities…") and is broader in scope in that the new language is not explicitly limited to cybersecurity-related risks/contractual requirements.
EX.CN-02: Expected cybersecurity practices for critical third parties that meet the risk management objectives of the organization are identified, documented, and agreed	**GV.SC-07**: The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship **GV.SC-05**: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	**EX.CN-02** refers to "critical third parties," and "expected cybersecurity practices of third parties," terms that are not used in Draft CSF 2.0.

Category #3—Monitoring and Managing Suppliers (EX.MM): *The risks posed by a third-party are monitored and managed over the course of the relationship*		
Proposed EX Subcategory	**Closest Analogs in Draft CSF 2.0**	**Substantive Differences**
EX.MM-01: Critical suppliers and third parties are monitored to confirm that they continue to satisfy their obligations as required; reviews of audits, test results, or other assessments of third parties are conducted	**GV.SC-07**: The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship **GV.SC-08**: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities **DE.CM-06**. External service provider activities and services are monitored to find potentially adverse events **ID.IM-02**: Security tests and exercises, including those done in coordination with suppliers and relevant third parties, are conducted to identify improvements	**EX.MM-01** refers to "critical suppliers," a term that is not used in Draft CSF 2.0.
EX.MM-02: Inter-dependent and coordinated cybersecurity risk management practices with	**GV.SC-07**: The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed,	**EX.MM-02** is more prescriptive, referring specifically to "inter-dependent and coordinated" C-SCRM practices

third parties are managed to ensure ongoing effectiveness	responded to, and monitored over the course of the relationship	

Category #4— Relationship Termination (EX.TR): *Relationship termination is anticipated, planned for, and executed safely*		
Proposed EX Subcategory	**Closest Analogs in Draft CSF 2.0**	**Substantive Differences**
EX.TR-01: The organization anticipates and plans for the termination of critical relationships under both normal and adverse circumstances	**GV.SC-10:** Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	**EX.TR-01** refers to "critical relationships," a term that is not used in Draft CSF 2.0.
EX.TR-02: Relationship terminations and the return or destruction of assets are performed in a controlled and safe manner	**GV.SC-10:** Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	**EX.TR-02** is more specific and prescriptive, as it refers specifically to "the return or destruction of assets." It is also broader in scope, as it requires the return/destruction of assets to be done in a "controlled" manner.