U.S. Chamber of Commerce

[redacted]

Via cyberframework@nist.gov

March 17, 2023

Alicia Chambers
Executive Secretariat
National Institute of Standards and Technology
Gaithersburg, MD 20899

Re: *Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework* (January 19, 2023)

Dear Ms. Chambers:

The U.S. Chamber of Commerce welcomes the opportunity to comment on the National Institute of Standards and Technology's (NIST's) *Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework* (the *Concept Paper*). It outlines potential, important changes to the Cybersecurity Framework (the CSF or the Framework) Version 1.1 to solicit public consideration and feedback.[1] NIST is off to a productive start in updating the CSF and engaging the business community. NIST's step-by-step approach to both summarizing anticipated changes to the CSF and hearing from stakeholders is positive.

In responding to NIST's request for information (RFI)[2] on a revised Framework (i.e., CSF 2.0) in April 2022, the Chamber said that our main objective is for NIST to make essential and practical amendments to the CSF while keeping an updated version compatible with CSF Version 1.1. We noted that business groups are not pressing NIST to make substantial changes to the CSF. Instead, many are seeking assistance on topics such as how to better assess their cybersecurity progression along the CSF's 4 Tiers.

The Chamber added that as NIST considers updates to the CSF, many in industry urge the agency to stay consistent with its judicious treatment of cyber supply chain risk management matters. Meanwhile, NIST should work with industry to bring the Informative References up to speed to reflect the latest cyber work products and thinking in this complex area.

[1] https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20
https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf

[2] NIST request for information, "Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management," *Federal Register*, February 22, 2022.
https://www.federalregister.gov/documents/2022/02/22/2022-03642/evaluating-and-improving-nist-cybersecurity-resources-the-cybersecurity-framework-and-cybersecurity
https://www.nist.gov/cyberframework/comments-received-rfi-about-evaluating-and-improving-cybersecurity-resources

Key Points

- The Chamber urges NIST to make practical improvements to the CSF while keeping an updated version compatible with CSF Version 1.1. The Chamber welcomes NIST's plan to publish a draft CSF 2.0 this summer and hold at least one in-person workshop before finalizing an updated version.

- The Chamber agrees with NIST's view that the CSF Core should remain high level and concise, and only a small number of notional implementation examples should be included.

- The Chamber does not anticipate NIST incorporating the Cybersecurity and Infrastructure Security Agency's (CISA's) Cross-Sector Cybersecurity Performance Goals (CPGs) in the CSF Core. Nonetheless, we urge NIST to resist any requests to add them.

- NIST indicates that it will produce an optional template for developing CSF Profiles. Many organizations may find a model Profile useful. NIST should continue emphasizing that there is a wide variety of Framework Profiles, not only among sectors but within sectors. NIST should also continue to stress that the Framework does not prescribe Profile templates, thus enabling flexibility in an organization's use of the CSF.

- Some business groups disagreed about whether to add a new Govern Function to the CSF, including the operational, policy, and security advantages and disadvantages of a Govern Function. Also, further discussion is needed on what content should populate a Govern Function.

- The Chamber recommends that NIST revise the five Identify/supply chain Subcategories, which were last written in 2018. NIST could help users of the CSF prioritize and/or narrow the suppliers and third-party partners that need to be engaged in a cyber supply chain risk management (C-SCRM) process. NIST is urged to refrain from (1) further integrating C-SCRM outcomes throughout the CSF Core and (2) creating a new Function focused on C-SCRM.

- The Chamber recommends that NIST consider including a new Tier, such as Managed, that could be incorporated between Tier 3 Repeatable and Tier 4 Adaptive.

The remainder of this letter consists of business community feedback, which ranges from high level to specific, that the Chamber has received in response to NIST's *Concept Paper* and the NIST-led working sessions, which were held on February 22 and 23, 2023.

1. Relationship to Standards and Mappings/Informative References

According to the *Concept Paper*, NIST is planning to include some updated special publications (SPs) and one standard in the CSF's Informative References. Here are four items that NIST should consider incorporating:

- NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (SP 800-53 Rev. 5, as of December 2020).[3]

- NIST Special Publication 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities* (SP 800-218, as of February 2022).[4]

- NIST Special Publication 800-161, Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (SP 800-161 Rev. 1, as of May 2022; rev. 2 is pending).[5]

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2022.[6]

2. CSF Core Changes

The Chamber concurs with NIST's view that the CSF Core needs to remain high level and concise. One company indicated to the Chamber that the Identify Function could be refreshed in targeted ways. "There are Subcategories in various parts of the CSF Core, such as those related to auditing, that could probably be consolidated in the Identify Function." An example of the approach follows:

Function	Category	Subcategory [Notional examples]	Informative References
ID		**ID.SC-4:** 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. [p. 28] **PR.AC-1:** Identities and credentials are issued, managed, verified,	

[3] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[4] https://csrc.nist.gov/publications/detail/sp/800-218/final
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

[5] https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
https://csrc.nist.gov/News/2021/2nd-draft-sp-800-161-rev-1-cscrm-practices

[6] https://www.iso.org/standard/82875.html

		revoked, and **audited** for authorized devices, users, and processes. [p. 29] **PR.PT-1: Audit**/log records are determined, documented, implemented, and reviewed in accordance with policy. [p. 36]	

Participants at the CSF 2.0 workshop on February 15, 2023, suggested that CISA's CPGs could "complement" the CSF.[7] The Chamber strongly believes that the CPGs—which seem to have a regulatory bent according to the *National Cybersecurity Strategy*—should be limited to complementing the CSF and avoid competing with it.[8]

Perhaps in contrast to the CPGs, Framework users consistently highlight numerous ways in which the CSF has been effective in helping organizations understand and manage their cybersecurity risks. Key desired attributes of the CSF include its flexible, simple, and voluntary nature—which have been beneficial for implementation by organizations of varying sizes and sectors.[9] The Chamber does not anticipate that NIST plans to incorporate the CPGs in the CSF Core because stakeholders have not asked for it.[10] Still, we urge NIST to resist any new requests to do so.

3.0 CSF Guidance and Profiles

The *Concept Paper* indicates that CSF 2.0 will include updated and expanded guidance on Framework implementation. NIST notes that it intends to include notional implementation examples of concise, action-oriented processes and activities to help organizations achieve the outcomes of the CSF Subcategories and the guidance provided in the Informative References.

- The Chamber **agrees** with NIST's view that the CSF Core should remain high level and concise, and only a small number of notional examples should be included.

[7] https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-workshop-2

[8] https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[9] NIST, *Initial Summary Analysis of Responses to the Request for Information (RFI)—Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management*, June 3, 2022.
https://www.nist.gov/system/files/documents/2022/06/03/NIST-Cybersecurity-RFI-Summary-Analysis-Final.pdf

[10] Ibid.

- The Chamber **agrees** with NIST's thinking that a small list of examples should not be construed as a comprehensive list of all actions that could be taken by an organization to meet CSF outcomes. Nor would they represent a baseline of required actions to address cybersecurity risks.

NIST says that it welcomes feedback as to whether these implementation examples should be added as a column included within the CSF Core, perhaps modeled after NIST publications such as the *Secure Software Development Framework* (SSDF).[11] The Chamber thinks NIST has something in mind that resembles what is shown in the table below. This intentionally simple approach—which the Chamber puts forward for discussion rather than endorsement—is modeled after the first rows in Table 2 on p. 24 of the CSF and Table 2 on p. 5 of the SSDF.

Function	Category	Subcategory	Notional Implementation Examples	Informative References
ID	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	**Example 1:** TBD **Example 2:** TBD **Example 3:** TBD	**CIS CSC 1** **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5

In addition, the *Concept Paper* says that many responses to NIST's RFI called for a template to help organizations develop CSF Profiles. NIST indicates that it will produce an *optional* template for developing CSF Profiles. Many organizations may find a model Profile useful.

The Chamber urges NIST to continue emphasizing that there is a wide variety of Framework Profiles, not only among sectors but within sectors. The Chamber recognizes that NIST already stresses that the "Framework does not prescribe Profile templates," thus enabling

[11] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

flexibility in an organization's use of the CSF.[12] Nonetheless, a cautionary message is still needed for stakeholders, including some policymakers.

A number of stakeholders may not fully appreciate that a Profile represents the *alignment* of the Functions, the Categories, and the Subcategories *with* an organization's business requirements, risk tolerance, and resources. All these factors can vary greatly, not only among private organizations but within the divisions of a single firm. In other words, Framework Profiles do not lend themselves to one-size-fits-all cyber risk management goals, solutions, and outcomes.

4. Cybersecurity Governance

On February 22, 2023, the Chamber attended the NIST working session on cybersecurity governance. The two main takeaways appeared to be the following:

- NIST representatives said that they plan to create a new Govern Function in CSF 2.0. However, the Chamber asked whether there is a consensus to move forward on a new Govern Function, owing to the fact that business opinion on this subject is unsettled. It seems that the operational, policy, and security pros/cons related to a Govern Function still need to be fully addressed.

- Attendees at the working session on cybersecurity governance, including those who advocated for a Govern Function in their responses to the 2022 RFI, were uncertain about what content should populate a Govern Function. Some association representatives stressed that the Govern Function should not "get too big" or that NIST should not "add more" to it, but there was seemingly no agreement on what content should populate a Govern Function.

In the Chamber's discussions with business groups, a number of them expressed disagreement that a new Govern Function should be included inside an updated CSF. On the one hand, some firms and associations believe that a Govern Function would complement their current activities and add value to the CSF.

On the other, one company told the Chamber that adding a new Govern Function "would completely change" the face of the CSF. "Governance is already threaded throughout the Framework." More specifically, a Govern Function "can mean a lot of different things to different audiences. It is an invitation to regulation," the company cautioned. A sector association noted that it is reluctant to add a Govern Function because it "will open a can of worms—that is, establishing a new Function would create more problems [e.g., in the area of regulation] than it would correct."

Business groups thoughtfully discussed the pros and cons of a new Govern Function, seemingly the one proposal of the *Concept Paper* that generated the most debate. A selection of the points raised are provided in the following table.

[12] https://www.nist.gov/cyberframework/examples-framework-profiles

Select Pros and Cons of a New Govern Function

Pros

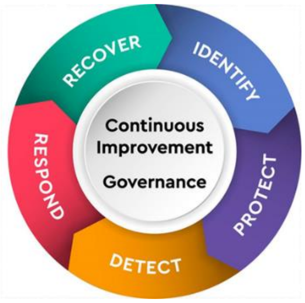
- The management of risk is foundational to all cybersecurity programs. Providing an expanded emphasis on risk management within a new Govern Function, which NIST proposes, could benefit Framework users.
  - For sizable or mature organizations, the addition of a new Govern Function could validate or enhance their existing cyber risk governance activities.
- Greater emphasis should be placed on governance in laying the foundation of a strong and resilient cyber ecosystem. There can be a tendency among some organizations to gloss over the key governance activities under the Identify Function.
- Cybersecurity governance—which generally refers to the development and implementation of an organization's program(s) and activities to enable an ongoing understanding and management of its cybersecurity risk—must be inwardly focused and not driven by regulation.
  - A Govern Function should emphasize to policymakers that use of the CSF—or any comparable cybersecurity frameworks, standards, and industry-led best practices—for regulatory purposes must come with strong liability protections for CSF users.[13]
- Additional arguments favoring the creation of a new Govern Function are articulated in section 4 of the CSF 2.0 *Concept Paper*.[14]

Cons for a Govern Function

- The current five-Function model of the CSF is widely embraced because of its straightforwardness and applicability to all types and sizes of organizations.
- The term "governance" can be applied to all the controls of a cybersecurity program. Creating an explicit Govern Function focused on specific areas could diminish that broader meaning. As an example, the following graphic is used by some organizations to illustrate Governance as a core concept for the entirety of the CSF in connection with Continuous Improvement.

[13] The Chamber believes that policymakers should stand behind the perceived correctness of their regulations. Anything short of clear liability protections for private entities would call into question the assumption that the cybersecurity requirements are appropriately risk based, technically sound, and workable.

[14] https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf



- Creating a Govern Function, as articulated in the NIST *Concept Paper*, would add unnecessary complexity to the CSF and could deter further use of the Framework. This could be the case especially for organizations that have less mature and minimally funded cybersecurity programs.

- Regardless of their size or security sophistication, many organizations base their cybersecurity programs on the CSF, which may include some form of reporting (e.g., on measurements and status updates) to business executives and boards of directors. Changing the foundation of the CSF by adding a sixth Function as an overlay would complicate such activities.

- The elevation and expansion of governance-oriented Subcategories, which currently reside in the Identify Function, could result in an overemphasis on those topic areas.

    - Some of the arguments favoring a new Govern Function focus on shifting existing CSF provisions within the Identify Function to the Govern Function and then expanding them. Others argue in favor of adding relevant topics from other NIST publications. Such moves could unintentionally enlarge the CSF, diminishing its historically broad appeal.

- Increased coverage of governance should be done within the current Function areas of Identify and Protect rather than establishing a new Function.

- Governance should arguably include managing the supply chain security of business partners, but such thinking is not expected to be reflected in a new Govern Function, which lessens arguments favoring a Governance Function. Indeed, the expansion of supply chain security activities can—and should—be managed within the existing Functions, which is the more appropriate way to update the CSF.

- There is notable concern among many businesses that an elevated Govern Function could make the Framework a regulatory tool in the hands of government authorities.[15] Such concerns are legitimate. Both federal and state agencies have taken advantage of cybersecurity governance to help frame and issue new and prescriptive regulations. Here are two examples:

[15] The term "governance" is adapted from a related NIST definition. https://csrc.nist.gov/glossary/term/govern_pf

- The Securities and Exchange Commission's proposed cybersecurity incident disclosure rules would require an unprecedented micromanagement of companies' cybersecurity governance.[16]

- The New York Department of Financial Services' second amendment to its Cybersecurity Regulation, which governs cybersecurity requirements for certain financial services companies, would add extensive and prescriptive requirements in the area of cybersecurity governance.[17]

Nonetheless, the *Concept Paper* puts forward the key changes that NIST has in mind for CSF 2.0. The current Categories in the CSF that cover governance—such as Business Environment (ID.BE), Governance (ID.GV), and Risk Management Strategy (ID.RM)—would likely be moved into the Govern Function.

The *Concept Paper* adds that the current Subcategories under Identify/Governance (ID.GV)—such as cybersecurity policy (ID.GV-1), cybersecurity roles and responsibilities (ID.GV-2), legal and regulatory requirements (ID.GV-3), and governance and risk management processes (ID.GV-4)—would probably be elevated to separate categories under a new Govern Function. Below, the Chamber attempts—for discussion purposes only—to capture elements of NIST's objective regarding the Govern Function. It is modeled after Table 1 on page 23 of the CSF.

Function Unique Identifier	Function	Category Unique Identifier [Examples]	Category [Examples]
GV	Govern	Current ID.GV	Governance
		GV.BE	Business Environment
		GV.RM	Risk Management Strategy
		GV.SC	Supply Chain Risk Management

[16] https://www.federalregister.gov/documents/2022/03/23/2022-05480/cybersecurity-risk-management-strategy-governance-and-incident-disclosure
https://www.sec.gov/comments/s7-09-22/s70922-20128398-291304.pdf
https://www.sec.gov/comments/s7-09-22/s70922-20132693-303184.pdf

[17] https://www.dfs.ny.gov/industry_guidance/cybersecurity
https://www.dfs.ny.gov/system/files/documents/2022/10/rp23a2_text_20221109_0.pdf
https://www.dfs.ny.gov/system/files/documents/2022/10/rp23a2_sapa_20221109.pdf

5. Cybersecurity Supply Chain Risk Management (C-SCRM)

According to the *Concept Paper*, NIST believes that CSF 2.0 should include additional C-SCRM-specific outcomes to help organizations address these distinct cyber risks. The Chamber recommends NIST revise the five ID.SC outcomes or narratives, which were last written in 2018. For example, NIST could help users of the CSF prioritize or narrow the suppliers and third-party partners that need to be engaged in a C-SCRM process.

- NIST should **refrain** from further integrating C-SCRM outcomes throughout the CSF Core across Functions.

- NIST should **avoid** creating a new Function focused on outcomes related to oversight and management of C-SCRM.

6. Assessment and Measurement

NIST says that the assessment and measurement of cybersecurity risk management programs and strategies continue to be an important area of the CSF. The Chamber agrees with RFI respondents who seek additional CSF guidance to support assessing and measuring an organization's use of the CSF. We appreciate NIST's intention to explain how organizations can use the Implementation Tiers and how they relate to measurement.

The Chamber urges NIST to consider including a new Tier, such as Managed, that could be incorporated between Tier 3 Repeatable and Tier 4 Adaptive. The movement between these two Tiers is quite significant in comparison with the lowest ones, which can lead some organizations to inflate their risk management postures when determining their standing against the Tiers.

CSF 1.1 (See pp. 8–11)	Tier 1	Tier 2	Tier 3	Tier 4	
	Partial	Risk Informed	Repeatable	Adaptive	
CSF 2.0 (Notional)	Tier 1	Tier 2	Tier 3	*Tier 4*	Tier 5
	Partial	Risk Informed	Repeatable	Managed	Adaptive

***

Thank you for the opportunity to provide NIST with comments on the *Concept Paper*. If you have any questions or need more information, please do not hesitate to contact Matthew Eggers [redacted].

Sincerely,

Matthew J Eggers

Matthew J. Eggers
Vice President
Cyber, Space, and National Security Policy Division
U.S. Chamber of Commerce