U.S. Chamber of Commerce

[redacted]

November 2, 2023

Via cyberframework@nist.gov

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

Re: Public Draft of the NIST Cybersecurity Framework 2.0

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) public draft of the Cybersecurity Framework (the CSF or the Framework) 2.0.[1]

The Chamber strongly supports the draft Framework, and we believe that businesses and policymakers see the joint industry-NIST Framework as a pillar for managing enterprise cybersecurity risks and threats, including at home and increasingly internationally. NIST has done an admirable job convening many organizations to develop the Framework, including revising it several years ago and, more recently, writing CSF 2.0.

Comments on the Draft CSF 2.0

The remainder of this letter consists of business community feedback, which ranges from high level to specific, that the Chamber has received on the draft Framework. The Chamber does not necessarily endorse each view, but we believe that NIST should consider each in the context of cybersecurity stakeholders' comments. In the following table, additions and strikethroughs are provided in blue text:

Section	Text	Recommendation
Page 3, line 142	"The Framework is forward-looking and is intended to apply to future changes in technologies, ~~and~~ environments, maintenance, and operations."	Maintenance and operations should also be referenced as this specifically calls out the spectrum of applicability for the CSF.

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

Page 11, line 394–395	". . [T] Target Profile should be updated to reflect changes in the organization and its realized cybersecurity risk."	"Realized" would add clarity that the cybersecurity risk has actually occurred.
Page 40	"DE.CM-06: External service provider activities and services are ~~monitored~~ overseen to find potentially adverse events . . ."	Removing "monitor" would alleviate conflicts associated with current monitoring policies (e.g., employee) at the federal and state levels.

Implementation Examples

Page 5, section GV.RM-07 [implementation examples]	"Strategic opportunities ~~(i.e., positive risks)~~ are identified and included in the organizational cybersecurity risk discussions"	The term "strategic opportunities" is clear, but the subcategory of "positive risks" should be removed as it is an insufficient description and counterintuitive.
Page 17, section ID.RA-05	"Threats, vulnerabilities, likelihoods, ~~and~~ impacts, and the Current Profile are used to determine risk and inform risk prioritization"	The Current Profile should be used as context for this analysis.
Pages 19–20, section ID.IM-03	"Lessons learned during execution of operational processes, procedures, safeguards, and activities are used to identify improvements . . ."	Refer to page 10 of the main document under the subheading 3.1.1 "Ways to Use Profiles." The second bullet refers to practices as safeguards: "Document the Informative References (e.g., standards, guidelines, and policies) and the **practices (e.g., procedures and safeguards)** [bolding added] currently in place and planned in the future[.]" Since practices are defined as safeguards, safeguards should be part of the lessons learned.

The Chamber received some mixed views on the draft implementation examples, less out of concern for NIST's approach to the CSF but because of how policymakers may seek to use—or *misinterpret*—the CSF.

First, an organization shared with the Chamber, "One of our key arguments since the Concept Paper was released in January 2023 has been that in order to preserve the flexible intent of the CSF, we need to keep the focus on the *what* [to manage] not the *how* [to manage]. The update of the CSF represents a significant shift from reactive to proactive cybersecurity practices. It also reflects the government's appetite for greater regulation of businesses to mitigate cybersecurity risk through governance as well as the addition of supply chain risk management requirements."

"While not law," the organization said, "the CSF seems to set a comparatively high bar for proactive steps to take for cybersecurity. And, if we aren't careful, the implementation examples (and so forth) could be incorrectly interpreted as *the bar* and leveraged as requirements in [federal] contracts."

This organization went on to emphasize that "the value of the CSF has been its flexibility; it's not meant to be prescriptive. The inclusion of the implementation examples and other cross-references could detract from the CSF's adaptability in the face of new threats, preventing it from being interpreted as a single, dynamic framework. In our organization's view, the implementation examples should be understood as separate from the CSF and strictly viewed as a guide for how the CSF *may* be implemented. Simply put, NIST should not link to the implementation examples the way that it has. Doing so would create an incorrect impression about how the CSF should be viewed by government agencies. Our organization raised this point to NIST at the September 2023 workshop."

The organization added, "Here's a potential scenario: If our organization were audited by the Department of Justice under a civil enforcement action, the department could unfairly use the implementation examples against us, saying that the examples 'show how we should be doing cybersecurity.' Even cybersecurity experts can disagree vigorously over the soundness of certain controls and their economic trade-offs."

Second, one firm stated, "We should ensure that CSF 2.0 remains a voluntary framework that does not turn into a mandate or compliance document like the Secure Software Development Framework (SSDF).[2] Further, NIST asked for industry input on how the other frameworks—such as the AI Risk Management Framework, the Privacy Framework, and the SSDF—should be incorporated or cross-linked." The firm added, "NIST has done a fairly good job of acknowledging the interrelated frameworks while staying in its lane. However, NIST will need to eventually address whether an umbrella framework is necessary to better link everything together along with corresponding controls."

[2] https://csrc nist.gov/Projects/ssdf

Third, echoing similar themes, another industry entity commented that "NIST has gone out of its way to reinforce the principle that the CSF is a framework that is principles-based and not prescriptive. A lot of businesses struggle to figure out how to implement the CSF, so the examples, footnotes, and references will probably be very useful for those firms that need a clearer path for implementation."

Fourth, a company said that while NIST "did not add a new function for supply chain risk management, we are concerned about the amount of attention that supply chain risk management is getting in the U.S. government and foreign governments, including the reporting requirements that potentially come with these things. Our company does not have a specific ask for the CSF but want to flag that this is an ongoing area of concern." The company added, "In addition to potential new reporting to a government, this trend is prompting extreme asks from some customers, such as assertions that software code has no known vulnerabilities."

Further, the company said, "It would be useful for the CSF to note that there are different types of risk, particularly that not all risk (e.g., systemic) can be mitigated. Section 3 seems like the best place for this statement. Unfortunately, [our company doesn't] see discussion of these types of risk in NIST's 800-30 or -37 publications and is unsure of an appropriate reference. We're open to other viewpoints on this topic."[3]

Fifth, an association told the Chamber, "Several small providers have indicated that the examples are helpful, although we understand the concern raised about the possibility of the [federal] government using the examples to conclude that a company did not meet certain expectations. While the CSF clearly states that the guidelines are intended to be scalable and/or adaptable to each individual framework user, the fact that the FCC and NTIA through BEAD[4] require companies to implement C-SCRM [cybersecurity and supply chain risk management] plans that include the CSF makes this concern possible.

"Furthermore, the FCC has required certain providers to prepare C-SCRM plans that include CISA's Cybersecurity Performance Goals (CPGs).[5] The CPGs also contain examples and link to the CSF. As a result, we would welcome further affirmation from NIST that the CSF examples are not prescriptive but, rather, only for guidance if needed."

---

[3] NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments, September 2012.
https://csrc nist.gov/pubs/sp/800/30/r1/final

NIST SP 800-37 Rev. 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, December 2018.
https://csrc nist.gov/pubs/sp/800/37/r2/final

[4] https://broadbandusa.ntia.doc.gov/sites/default/files/2022-05/BEAD%20NOFO.pdf (See p. 70.)

[5] https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

Sixth, a business told the Chamber, "We think that the cross-references and implementation examples are critical to helping smaller institutions with CSF implementation. Perhaps NIST can clarify the voluntary nature of these items. But we think it would weaken the nation's overall security posture if there isn't more clarity provided through such implementation examples."

Here are three points worth highlighting, the business said—

- "Guidance, not requirements: The CSF provides cross-references and implementation examples in response to many organizations, small and large, seeking to understand potential ways to implement the principles, not directives, which dictate specific measures." The draft CSF 2.0 explicitly notes, "The examples are not a comprehensive list of all actions that could be taken by an organization to achieve an outcome, nor do they represent a baseline of required actions to address cybersecurity risk."[6] This should reassure organizations that the CSF is still a risk and principles-based guidance and not a prescriptive set of actions to meet the principles.

- "Enhanced clarity: Cross-references and implementation examples aid organizations, regardless of their cyber maturity, to understand and apply the framework concepts. These examples are particularly beneficial for entities that might not have deep cyber expertise or resources. They give entities a starting point or a point of reference rather than a roadmap to be rigidly followed.

- "Flexibility through illustration: The cross-references and examples can be seen as illustrations of the concepts within the CSF in action; they provide clarity without compromising flexibility. Organizations can choose to follow, modify, or disregard the implementation examples based on their unique needs, situations, or challenges. Rather than being limiting, implementation examples should be viewed as tools to enhance the adaptability of the CSF by demonstrating its versatility."

***

Thank you for the opportunity to provide NIST with comments on the draft CSF 2.0. If you have any questions or need more information, please do not hesitate to contact Matthew Eggers [redacted].

[6] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf, p. 7.

Sincerely,

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