U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

Via CSF-SCRM-RFI@nist.gov

April 25, 2022

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

Re: NIST Cybersecurity Request for Information (RFI)

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) RFI, *Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management*.[1]

Broad swaths of the business community support the popular Cybersecurity Framework (CSF). The Chamber values the thoughtful and considerable effort that NIST has put into writing and updating it since 2013.[2] The Chamber's goal, which we believe that NIST shares, is to make key amendments to the CSF while keeping an updated version (i.e., a forthcoming CSF 2.0) compatible with CSF version 1.1.[3] The Chamber urges NIST to publish a draft CSF 2.0 so that groups can offer the agency feedback, including holding at least one workshop, before finalizing an updated version.

Key Points

- The Chamber's main objective is to make essential and practical amendments to the CSF while keeping an updated version (i.e., CSF 2.0) compatible with CSF version 1.1. The Chamber urges NIST to publish a draft CSF 2.0 so that groups can offer the agency comments and hold at least one workshop before finalizing an updated version.

- Business groups are not pressing NIST to make major 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.

- As NIST considers updates to the CSF, industry urges the agency to stay consistent with its judicious treatment of cyber supply chain risk management matters. Yet 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.

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 RFI. Unless otherwise stated, the Chamber does not necessarily endorse each view, but we believe that NIST should receive each one as part of stakeholders' comments. Also, the Chamber's letter addresses many of NIST's 14 topics that come under 3 main headings that the agency asks groups to address.

USE OF THE NIST CYBERSECURITY FRAMEWORK

1. The usefulness of the CSF for aiding groups in organizing cybersecurity efforts via the five functions in the CSF and actively managing risks using those five functions.

A computer software and technology corporation (the software corporation) shared with the Chamber that it has integrated the CSF into its enterprise risk management program. "The CSF influences the company's security risk culture and informs how we communicate our security capability maturity to senior management and the board of directors. The CSF is viewed as an external best practice that applies across our company's key services and various risk management roles. The CSF enables a conversation among practitioner and management teams who have differing areas of commercial focus and expertise. The CSF also functions as one of several approaches that our enterprise risk management program uses to validate cybersecurity across its company."[4]

Further, in its conversations with customers, partners, and other industry stakeholders, the software corporation has learned that its positive experience with the CSF is not unique. "Since 2014, the CSF has gained broad recognition as effective guidance for cybersecurity risk management. The CSF's broad applicability across sectors and organizations of different sizes has been critical to its success. Likewise, the CSF enables organizations to assess cyber risks, while accommodating their specific concerns, risk tolerances, and resources. The CSF's flexibility—combined with its focus on enabling informed security investments over time—supports continuous learning and improvements in organizations that use it."

A defense contractor conveyed, "Our company has assessed and mapped its information security organization to the five functions outlined in the CSF. Our information security directors have been assigned to these five areas, and managers have been assigned to specific subcategories. Each person understands his or her responsibilities for cybersecurity."

A cybersecurity solutions company noted, “Another advantage of the CSF is its flexibility. It can be overlayed to existing risk management processes to complement and improve them.”

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

A plastics, chemicals, and refining company (the plastics company) told the Chamber that “the CSF is not formally implemented at our business because we use ISO/IEC 27001. However, ISO/IEC 27001 is a risk-based standard that covers all or most NIST cybersecurity and related publications.”

An energy firm said, “Combining the answers to questions 1 and 2, our business uses the CSF as the foundation of its cybersecurity program. Virtually all company cybersecurity activities are mapped to the CSF, including our cybersecurity strategy and external benchmarks, which are shared with the board of directors. The benchmarks are provided in terms of the 4 CSF tiers, and we set tiering targets to drive strategic security objectives.”

The defense contractor noted, “We measure ourselves against the maturity of the CSF subcategories and roll up the aggregated scores to the category and function levels. We are then able to compare ourselves with the maturity of other defense firms.”

The defense contractor added, “In terms of improvements, we would recommend a change to the CSF’s maturity level definitions. As an example, our company uses the maturity scores that are aligned with the Software Engineering Institute Capability Maturity Model (SEI-CMM) levels rather than NIST CSF tiering or maturity scores. We have found that peer companies in our sector use nearly the same SEI-CMM-based definitions for their maturity levels. In contrast, NIST maturity level definitions are not as common or well known within the defense industry.”

A technology and software company (the T&S company) mentioned that “the CSF is purposely not providing users with maturity levels. Our company recommends that maturity levels be downplayed. The point made by the mobile communications firm under question 3 better tracks with our organization’s view.”

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

The plastics company noted, “The CSF is U.S.-based, and we are a global company. ISO/IEC 27001 is globally recognized.”

According to a mobile communications company, “CSF section 2.2 states that ‘Tiers do not represent maturity levels’ [p. 9],[5] but the CSF gives no reference to how it can be married to maturity models. The statement (i.e., ‘Tiers do not represent maturity levels.’) creates some confusion because many auditors/assessors label an assessment of an enterprise against the CSF core as a NIST cyber maturity assessment.” The company added that auditors/assessors “attest to the maturity of an organization’s cyber practices on a scale of 1–4 in alignment with the CSF tiers. Clarification surrounding these issues would be welcome.”

The defense contractor said, “One of the biggest challenges organizations may face is a lack of training. The NIST website provides information and case studies, but it may be difficult to apply them to a specific organization. Also, NIST developed the CSF to be flexibly applied to a range of organizations, but this can result in different interpretations of some areas. Within our organization, we have spent a significant amount of time and resources to understand and apply certain subcategories.”

The defense contractor noted, “The informative references that NIST provides vary in terms of clarity and usefulness. For example, our company is still assessing how to apply ID.BE-1 and -2 [p. 29] with respect to assigning ownership and rating maturity. We also find that suppliers that do not have a dedicated cybersecurity and/or IT support team will have challenges in implementing the CSF. These suppliers typically look to basic security and apply higher-level security controls depending on the product or service they provide. Or they will depend on a third-party provider’s interpretation of what controls are required. Also, NIST is largely viewed as a U.S.-centric control framework, which may create issues with international suppliers that must follow their respective governments’ cybersecurity requirements.”

The cybersecurity solutions company said, “Alternatively, the CSF can show examples of widely accepted maturity levels relevant to the tiers. This helps the CSF remain flexible and independent of specific standards or best practices. Such an approach is especially important for an organization that has established and matured its risk management process based on other standards or guidelines. It can be a challenge to increase an organization’s resources to both understand and overlay the CSF to an existing risk management system.”

4. Any features of the CSF that should be changed, added, or removed. These could 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 CSF; or references to critical infrastructure versus the CSF's broader use.

The mobile communications company expressed the following points to the Chamber on potential adjustments to the CSF. First, "NIST should add an additional tier—such as 'managed'—between tier 3 (repeatable) and tier 4 (adaptive). 'Managed' would help an organization determine where it sits between the two tiers. As it stands today, there seems to be a significant jump from tier 3 to tier 4, causing many organizations to perhaps inflate their profile. One possible outcome is a misrepresentation of an organization's actual standing against the tiers that the CSF defines," the company noted. Second, "NIST should consider updating the informative references to cover all the CSF subcategories and include the controls in NIST 800-53 controls and CMMC [the Cybersecurity Maturity Model Certification]."

The cybersecurity solutions company noted that "reverse mapping the NIST 800-53 controls to the CSF subcategories would be helpful. Mapping between the CSF and CMMC (e.g., NIST 800-171) would be extremely helpful too." The company added that it would welcome having NIST "elaborate further" on CSF section 4.0 (pp. 24–25), which pertains to self-assessing cybersecurity risk with the CSF.

The T&S company said that the CMMC should not be integrated into the CSF.

In its comments to the Chamber, the energy firm recommended the following considerations in updating the CSF:

- The CSF has an Awareness and Training category (p. 35) within the Protect function. A new subcategory should be added that includes cybersecurity training, the development of cybersecurity careers, and other techniques to help an organization manage its cybersecurity workforce.

- A planning subcategory within the Identify function (p. 28) should be added, as well as a second subcategory within the Protect function (p. 33) to facilitate the execution of organizational capability (OC) plans. Some entities use the OC term as a catch-all for having the appropriate staff and essential work processes, technologies, and partnerships to support the skills of their workforces. In a nutshell, OC is about having sufficient staff with the appropriate training to execute necessary work, such as cybersecurity.

- The Identify function subcategory ID.GV-3 (p. 30) instructs entities to understand and manage the cybersecurity legal and regulatory requirements, which should include policy advocacy. The role of advocacy (e.g., to improve legislation and regulations) should be expressly called out in CSF 2.0.

- The introduction of the CSF recommends that entities establish a current cybersecurity profile and a target profile (p. 2). Some organizations would welcome recommendations to close gaps between their current cybersecurity posture and their target state. NIST says that there are a variety of ways to use the CSF, and that decisions about how to apply it are left to the implementing organizations (p. 3). Still, there are perhaps ways for NIST to offer guidance on narrowing profile (p. 4) assessment gaps.

- The CSF does not address automation. NIST should consider situations where manual cybersecurity processes require automation.

- The CSF emphasizes assessing and managing cybersecurity risks (p. 31). The CSF, however, seems to miss the identification of new technologies in an evolving risk management environment. A new subcategory should be considered that addresses research on new technologies that may have short-term and/or long-term ramifications on an entity's risk management posture.

- The CSF does not describe building a cybersecurity risk management strategy or an architecture in much detail. A new category or subcategory—perhaps labeled Strategy, Asset Plan and Architecture—could be included in the CSF to help organizations develop and implement a cybersecurity strategy/architecture.

- The CSF's text on a risk management strategy could be fleshed out more. Proposed content includes—

    - Manage risk assessment and exceptions processes. Exceptions are used when an organization temporarily cannot mitigate an identified risk. The organization can petition the security organization to allow more time to implement a required mitigation; the petition should also include means as to how the organization would manage the risk during the interim. An alternative to exceptions is "acceptance" of the risk. Both are valid risk-management techniques, but we'd prefer "exception" to "acceptance" if there is any significant consequence to the risk.

    - Plan for processes to assess implementation of organizational measures and security controls. Risks may be treated by people, process, or technology. Many security controls tend to be implemented via technology, so "organizational measures" could cover things like clean-desk or acceptable-use policies, which tend more toward having a human (not a machine) read something and then an execution function. Indeed, if one broadens the definition of "security controls" to include people, process, and technology actions, then the inclusion of organizational measures may be redundant.

  - Develop an integrated risk management, or IRM, plan.[6]

  - Understand and document technology risks.

- The CSF should better accommodate DevSecOps—short for development, security, and operations—including more explicit references to secure software development. One outcome could involve revising or deleting "PR.DS-7: The development and testing environments are separate from the production environment" (p. 37). As with DevSecOps, there is a blurring (rather than a clear separation) of the development and production of software.

- Consider adding a new subcategory within the Protect function, Maintenance category (PR.MA): "Renew, retire, or replace technologies according to plan and in coordination with analysis and operational teams" (p. 40).

- Consider adding a new subcategory within the Respond function, Analysis category (RS.AN): "Provide forensics expert consulting" (p. 47).

The defense contractor told the Chamber, "We suggest that significant changes be made to PR.AC-1 ('Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes') [p. 33]. This is a very large subcategory, and it is impossible to effectively rate companies in a confident way. Whereas RC.CO-1 and -2 [p. 49] are very small, PR.AC-1 needs to be in a category of its own and some of the seemingly redundant detecting and incident response subcategories could be combined."

The defense contractor added, "More generally, the intent of the subcategories should be more explicit so that they are less subject to multiple interpretations across industry. By 'intent,' we mean what is the overall need for the subcategory or how does it apply. The CSF only provides the name of the subcategory and the informative references, which are not necessarily helpful to users. We recommend including 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 [p. 28], the CSF could clarify that this is for software, applications, and operating systems if this is the intent. To maintain the flexibility of the CSF, the description could start with 'Generally this subcategory means. ...' Above all, we recommend that any changes to the CSF should be incremental and not to such a degree that they would cause major alterations to our cybersecurity processes."

5. **Impact to the usability and backward compatibility of the CSF if the structure of the framework such as functions, categories, subcategories, etc. is modified or changed.**

Organizations such as the energy firm said that dramatic changes to the CSF could "disrupt a company's benchmarks that are based on the CSF." The energy firm noted that if categories/subcategories "are moved intact, then one could potentially manage the disruption. However, if the subcategories are split or combined, then an organization could lose the historical significance and continuity of past cybersecurity assessments."

The energy firm noted, "The supply chain risk management subcategories within the Identify function should be moved to more fitting areas of the CSF. For example, subcategories ID.SC-1 and ID.SC-2 [p. 32] should be under the categories of Risk Management Strategy (ID.RM) or Risk Assessment (ID.RA) [pp. 31–32]. Subcategories ID.SC-4 and ID.SC-5 (p. 33) should be housed within the Protect function [p. 33]."

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

The plastics company said, "The CSF is a starting point. The unique risk elements that an individual organization faces ought to be evaluated and treated. It's important that the CSF remains a guideline and does not become a regulation to be audited."

One commenter stressed that small and midsize businesses (SMBs) often have a challenge with "implementing many of the CSF's controls." The group urges NIST to promote a "CSF lite."

The Chamber thinks that NIST and SMBs should try to identify (e.g., in upcoming CSF workshops) what is specifically needed by many SMBs. The Chamber is aware of NIST's emphasis on providing tools aimed at SMBs, including NIST's Small Business Cybersecurity Corner webpage and NISTIR 7621 Revision 1, Small Business Information Security: The Fundamentals.[7] The apparent gap between what NIST offers and what some SMBs need would make for quality discussions.

A security consulting group told the Chamber it has views that may differ from other business organizations. "A key issue that we encounter is that businesses implement the CSF and believe it is more than just a starting point or a risk assessment tool. Some entities may have an incomplete "valuation of their overall level of cybersecurity and could have a false sense that they are doing as much as they should be doing."

The consulting group noted, “Our sense is that NIST 800-53 is overwhelming to many organizations. When the CSF was released, some organizations grabbed it as a replacement, instead of understanding the CSF’s strengths and weaknesses.” The group added that it “does not want the CSF to be turned into an auditing requirement,” but CSF users should be clear about what it is and what it is not.”

The consulting group put forward two recommendations for consideration in the CSF update effort:

- Consider ways to make the CSF’s outcomes more objective rather than subjective, such as improving the usefulness of the industry profiles, including the controls that organizations use to meet the subcategories, and gathering anonymized outputs from organizations that are categorized by industry for making comparisons and/or benchmarking purposes.

- Consider methods to improve guidance for organizations about how to meet expectations for some of the subcategories, such as baseline tasks that an organization should perform to satisfy a subcategory. Some of the subcategories are extremely large in scope (e.g., Asset Management (p. 28); and Identity Management, Authentication, and Access Control (p. 33)). Alternatively, if subcategories do not include expectations, the consulting group suggests that the informative references could be split into two categories to guide implementers:

    - NIST authoritative references with mappings into NIST 800-53/NIST 800-82.

    - Non-NIST informative references with mappings to other frameworks, standards, and authorities.

The consulting group added, “Since there is no context provided except the informative references, some implementers get confused and may use them incorrectly as authoritative. Also, NIST should consider how the performance goals that CISA [the Cybersecurity and Infrastructure Security Agency] is developing fit with the CSF. Perhaps they should be mapped to the subcategories or the informative references.”

The T&S company said that the consulting group’s suggestions could “move the CSF away from the CSF’s strengths and make it even more U.S.-centric. More feedback from industry is needed on these views before they are considered for inclusion in the CSF.”

The software corporation told the Chamber that “NIST should take a comprehensive look at what cybersecurity and supply chain risks mean today compared with when the CSF was updated in 2017 and 2018. NIST can both strengthen and foster a broader adoption of the

CSF by evaluating how flexible it is in responding to the constantly changing cybersecurity threat landscape. For instance, ransomware and supply chain risk management should be more integrated into the framework."

In addition, the software corporation said, "A more holistic approach is required to drive cohesion across the CSF and other NIST frameworks and guidance documents. NIST guidance that is used to supplement the CSF should not be bolted on but be complementary and integrated well. NIST has an opportunity to make improvements in how the CSF functions align with the functions in NIST's Privacy Framework and its draft Artificial Risk Management Framework.[8] More guidance is needed for practical implementation of the CSF, including how it can be used to develop tabletop exercises, playbooks, cloud security, and emerging technologies."

The software corporation said, "Additional guidance is needed to assist organizations in making the right tier determinations. Current tier definitions describe the state of an organization's risk management practices, integrated risk management program, and external participation (e.g., an information sharing group). Yet specific guidance is needed to assist product teams in determining whether their cybersecurity outcomes meet the state of risk management practices in each tier. For example, suppose that an organization sets its current profile at tier 2 and its target profile at tier 3 for all the CSF categories. What key markers can it use to ensure that its cybersecurity outcomes meet the expectations of the tier?" The software corporation said that NIST should "consider issuing guidance to assist an organization in gaining a solid understanding of what it takes to attain tier levels and have confidence in its determinations."

Furthermore, the software corporation noted, "Tiers 1–4 in the CSF do not currently allow organizations to account for continuous improvement over time within each tier. Suppose, for example, that a product team has attained a tier 2 for 3 consecutive years while continuously improving its cybersecurity practices (i.e., moving from level 3 to a notional 3.5). How would these improvements be monitored and acknowledged? The CSF does not account for such ongoing, marginal improvements using the 1 to 4 tiering model."

The software corporation argued that NIST should consider "enabling the tiers to account for continuous year-to-year improvement of cybersecurity risk management practices. One possible solution could be to create low, moderate, or high levels within each tier, accompanied by guidance on how to attain these levels. Alternatively, NIST could examine other models or issue guidance that fosters a more accurate monitoring of continuous improvement within the tiering structure."[9]

The defense contractor said to the Chamber, "We recommend that NIST provide clearer guidance on how companies should put together CSF profiles using a standardized approach. We recognize that NIST has developed a Cybersecurity Framework Manufacturing Profile Low Impact Level,[10] but the example is so complex that even a large manufacturing company faced difficulties understanding and adhering to it. We would welcome guidance on preparing profiles in a standardized way that is tailored to industry and by sector. Additional guidance is needed when it comes to using the same controls in different areas and not creating multiple profiles in the same company."

RELATIONSHIP OF THE CSF TO OTHER RISK MANAGEMENT RESOURCES

7. **Suggestions for improving alignment or integration of the CSF 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 CSF. These resources include the following:**

    - **Risk management resources such as the NIST Risk Management Framework,[11] the NIST Privacy Framework,[12] and Integrating Cybersecurity and Enterprise Risk Management (NISTIR 8286).[13]**

    - **Trustworthy technology resources such as the NIST Secure Software Development Framework,[14] the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline,[15] and the Guide to Industrial Control System Cybersecurity.[16]**

    - **Workforce management resources such as the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity.[17]**

The software corporation told the Chamber that the benefits of the CSF could be better optimized through "more cohesion with related NIST frameworks, SPs [special publications], and NISTIRs [NIST interagency reports]." Related, "Closer alignment and cohesion with the NIST privacy and AI frameworks would raise the question of whether the five functions in the CSF are sufficient." NIST should review whether additional functions present in other frameworks, such as the Privacy Framework, be included in CSF 2.0." The software corporation asked, "Why is there a governance function in the privacy and AI frameworks but not in the CSF?"

The cybersecurity solutions company said, "The CSF update effort should be viewed as an opportunity to improve alignment and integration of the CSF with other NIST risk management resources, especially the Risk Management Framework; the Privacy Framework; and NISTIR 8286, Integrating Cybersecurity and Enterprise Risk Management."

"In general, the more aligned and integrated the CSF is with the other NIST risk management resources, the better it can assist organizations in prioritizing their resources to improve cybersecurity. However, a key challenge that an organization may encounter is identifying the best way to integrate the subcategories of the CSF with controls or tasks defined in the other NIST risk management resources. Additional guidance would be welcome to help organizations achieve coherent integration of NIST resources," the cybersecurity solutions company added.

8. **Use of non-NIST frameworks or approaches in conjunction with the CSF. Are there commonalities or conflicts between the CSF and other voluntary, consensus resources? Are there commonalities or conflicts between the CSF and cybersecurity-related mandates or resources from government agencies? Are there ways to improve alignment or integration of the CSF with other frameworks, such as international approaches like the ISO/IEC 27000-series,[18] including ISO/IEC TS 27110?[19]**

The plastics company told the Chamber that "as a user of ISO/IEC 27001, it is fundamentally important that ISO conforms with the CSF."

The energy firm noted that it is constructive when some agencies—in partnership with industry—create CSF-based tools to help industry entities secure their systems. "From roughly 2017 to 2020, the Coast Guard worked with private organizations to write Navigation and Vessel Inspection Circular (NVIC) 01-20, Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities.[20] What's notable, the Coast Guard largely avoided crafting new, and possibly overlapping/conflicting, regulations. Instead, the agency mapped its regulations to the CSF." The energy company added, "Leveraging the CSF avoids the creation of overly prescriptive, one-off regulations—making it easier for regulated companies to implement/comply agency requirements because they are already mapped to something like the CSF, which a company may already use."

According to the defense contractor, "A strong alignment or an ability to connect like items would be beneficial when working with the supply chain. Suppliers of all sizes would have security principles of all sizes. Having the ability to connect like frameworks or related elements would help increase the fidelity of risk determinations and reduce organizations' workloads. We would also support increased alignment between the CSF and the ISO/IEC 27000-series. The ISO-based security at our suppliers is very common in the nongovernment technology and commercial areas, especially outside of the U.S. where NIST is considered a U.S.-centric tool."

The cybersecurity solutions company said, “The ISO/IEC 27000-series follows the defined structure of ISO management system standards, which is different from the CSF structure. Still, there are commonalities in that both tools recognize layered management structures and a set of controls/subcategories and require continuous improvement. NIST can encourage organizations that already implement ISO/IEC 27000-series to refer to ISO/IEC TS 27110 and take advantage of the CSF’s core to improve the implementation of controls.”

9. **There are numerous examples of international adaptations of the CSF 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 that any update increases the international use of the CSF?**

The plastics company commented, “The CSF, by its very nature, is oriented toward the U.S. Other frameworks (e.g., ISO/IEC 27001) are more internationally oriented. Much like how the British information security standard (BS7799) was eventually incorporated into the ISO standard, having CSF as an international standard would help companies that operate in a global economy.”[21]

The Chamber actively supports using the CSF at home and abroad. Multinational firms typically urge foreign governments and private organizations to use the CSF as a common driver for cybersecurity activities across multiple sectors. NIST has played a remarkable role in encouraging international participation and collaboration in CSF development and implementation processes. It should continue to push broader awareness of the CSF, including through public comment periods and workshops that account for international perspectives.

The T&S company added, “For an international approach to be truly effective, NIST should advocate for international documents that are based on the CSF or that can be easily mapped to it. While it is positive for other countries to claim that they are adopting the CSF, it is not clear how this translates into aligning cybersecurity approaches/requirements in practice. Without aligning approaches/requirements, companies are spending time and limited resources on complying with different, but marginally similar, programs rather than advancing security.”

The T&S company went on to convey that “NIST's current approach is helping increase adoption of the CSF for internal use by organizations, especially companies in the U.S. But if NIST wants to influence what customers/enterprises ask of their vendors in other countries, it is improbable that the CSF can be adopted much more than it is today. However, if NIST has meetings with organizations outside the U.S. and recommends wide adoption of documents that demonstrate international acceptance of the CSF, that would be a strong message and one that would be easier for others to get onboard with. What's more, NIST should continue to act as an advocate for its work in international standards organizations."

The defense contractor told the Chamber that "NIST should maintain a good mapping to the main cybersecurity international standards, such as the ISO/IEC 2700-series."

10. **References that should be considered for inclusion within NIST's Online Informative References Program (OLIR).[22] 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 CSF; the NIST Privacy Framework, Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53);[23] the NIST Secure Software Development Framework; and the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline.**

Comment pending.

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT

11. **National Initiative for Improving Cybersecurity in Supply Chains (NIICS).[24] 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 EO 14028,[25] to increase trust and assurance in technology products, devices, and services?**

The plastics company indicated that "NIST should consider encouraging [supply chain] customers and vendors to share risks, as well as suggest a common, recognized way of communicating base levels of security, which is similar to a SOC2,[26] of customers and vendors."

The software corporation told the Chamber, "Supply chains are a cross-cutting concern and impact products, devices, and services; they also impact the organizations and processes that produce them." The company added, "One of the biggest challenges an organization faces is learning how to approach the inherent complexity of supply chain risk management. NIST can help industry by providing guidance on how an organization can map its supply chain, what threats it faces, and the application of security controls based on existing NIST publications. This approach could help organizations make more manageable what can otherwise feel like an insurmountable challenge."

The defense contractor said, “One of the biggest challenges is how to get cybersecurity services to [SMB] suppliers, or any supplier who does not have a dedicated IT and dedicated cyber team. The cost for these companies to put a cybersecurity program in place is often significantly larger than the cost of the product or service they are providing to us.”

The cybersecurity solutions company commented, “To improve the trustworthiness of the supply chain, NIST should provide guidance regarding the definition and secure exchange of digital artifacts that assists the verification of supplier attestation. Similar to the CSF, such guidance should have flexibility to be overlaid to multiple standards, best practices and technologies.”

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.**

The software corporation commented to the Chamber, “While most approaches and tools tend to focus on individual organizations, many supply chain risk management engagements benefit from collaboration and transparency between suppliers and consumers. For example, group approaches, such as the Internet Engineering Task Force Supply Chain Integrity, Transparency, and Trust architecture, enable the secure and verifiable exchange of supply chain information between suppliers and consumers. Carrying this information throughout the supply chain would promote enhanced collaboration.”[27]

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?**

The software corporation noted, “Organizations and governments do not have contractual influence over open-source projects. Open-source projects are under no obligation to adopt contributions or process changes proposed by NIST. It would be useful to have guidance on compensating controls that open-source consumers can put in place to improve assurance (e.g., to address the Secure Software Development Framework criteria).”

14. **Integration of the CSF and Cybersecurity Supply Chain Risk Management Guidance.[28] Whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated CSF—or whether and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately developed by NIST.**

The mobile communications company said to the Chamber that supply chain considerations should be "limited to the CSF's informative references."

The cybersecurity solutions company said that the CSF should remain "voluntary guidance to address cybersecurity risks and threats in a comprehensive manner. To this end, tightly coupling the CSF with cyber supply chain risk management (SCRM) is not recommended."

The energy firm stressed, "NIST should not integrate supply chain risk management considerations into the CSF any more than is already there. A supply chain CSF profile with relevant informative references would be a better way to present this guidance."

The software corporation noted, "NIST 800-161 is a difficult document for stakeholders to consume because of its complex structure and length. By incorporating more supply chain risk management content into the CSF, the CSF can act as a guide to the relevant portions of NIST 800-161 for different categories and subcategories. It may also be possible to remove assessment process content from NIST 800-161 and instead defer to the assessment processes described in the CSF."[29]

A communications group stressed that NIST should approach changes to the cyber SCRM text in the CSF with prudence. Cyber SCRM is complex and varies considerably across both public and private organizations and sectors. Between 2017 and 2018, NIST expanded its guidance on using the CSF to address SCRM issues (see section 3.3 of the CSF). Also, the federal government has been active with legislative and executive branch SCRM initiatives in this area over the past several years.

As NIST contemplates updates to the CSF, we urge the agency to remain consistent with its judicious treatment of cyber SCRM matters. Still, NIST should work with industry to bring the informative references and related mappings up to speed to reflect the latest cyber work products and thinking in this complex area. All in all, NIST should steer away from adding a more detailed or prescriptive treatment of cyber SCRM issues to CSF 2.0. The joint NIST-industry CSF is not the optimal place to address in detail what some (e.g., policymakers) may misconstrue to be prescriptive controls or policy mandates.

It is worth highlighting the Chamber's thinking on cyber SCRM at some length. We believe that policymakers should not take advantage of the business community's support for the CSF to forge prescriptive pathways to cyber SCRM. Cyber defenses need to rely on industry best practices and reflect the efficient, decentralized architecture of companies' supply chains. An excerpt from the Chamber's April 2017 letter to NIST on updating the CSF is below.

Excerpt From the Chamber's April 2017 Letter to NIST on Updating the CSF

COMMUNICATING SCRM OBJECTIVES WITH SUPPLIERS AND PARTNERS

As recently as September 2016, the Chamber urged NIST to provide additional guidance concerning SCRM, which [CSF] version 1.1 does through the inclusion of new explanatory language in section 3.3. The Chamber's national Cybersecurity Campaign urges businesses to use the framework when communicating with partners, vendors, and suppliers about SCRM activities. Businesses of all sizes find it challenging to identify their risks and prioritize their actions to reduce weak links vulnerable to penetration, theft, and disruption.

The Chamber supports many efforts to enhance the security of public and private information and communications technology (ICT) networks and systems. The revised framework features SCRM considerations throughout the document. However, the Chamber wants to put the SCRM language in context.

First, it is important to highlight that businesses are linked together through a global web of interconnected, predictable, and efficient supply chains. U.S. businesses rely on these supply chains—which feature physical and digital characteristics—to access international consumers and compete in the global marketplace. The Chamber urges NIST and policymakers to recognize the complexity of mitigating cyber supply chain risk without compromising the interconnectivity that helps ensure the trade flows, access to markets, and the competitiveness of U.S. businesses.

Second, the Chamber urges policymakers to reject prescriptive and/or excessive SCRM programs that inject the United States or foreign governments directly into businesses' innovation and technology development processes, which are international in scope. Version 1.1 does not call for such regimes, which is positive, and this should not change in future frameworks.

Ambitious public- and private-sector efforts are under way to manage cyber supply chain risk. The Chamber opposes government actions that would create U.S.-specific guidelines, set private sector security standards, or conflict with industry-led security programs. Instead, cybersecurity stakeholders should seek to leverage consensus-based international agreements that enable ICT manufacturers to build products once and sell them globally. The revised framework is constructively consistent with such a view.

Third, the Chamber has a fundamental concern about policies that could broadly apply restrictions on international commerce based on real or perceived threats to the cyber supply chain and ICT products' country of origin. ICT cybersecurity policy must be geared toward embracing globally recognized standards, facilitating trade, and managing risk. NIST understands industry's core apprehension in this area, but we want to draw the attention of Congress and agencies to industry's position.[30]

***

The Chamber appreciates the opportunity to provide NIST with comments on its cybersecurity RFI. If you have any questions or need more information, please do not hesitate to contact Christopher Roberti [redacted] or Matthew Eggers [redacted]

Sincerely,

Matthew J Eggers

Christopher D. Roberti
Senior Vice President
Cyber, Intelligence, and
and Supply Chain Security
U.S. Chamber of Commerce

Matthew J. Eggers
Vice President
Cybersecurity Policy
U.S. Chamber of Commerce

Endnotes

[1] https://www.federalregister.gov/documents/2022/02/22/2022-03642/evaluating-and-improving-nist-cybersecurity-resources-the-cybersecurity-framework-and-cybersecurity

[2] The U.S. Chamber of Commerce, “One and Done? Not for NIST and the Cyber Framework.” April 16, 2018.
https://www.uschamber.com/security/cybersecurity/one-and-done-not-nist-and-the-cyber-framework

[3] The Chamber assumes that many readers of this letter have a working familiarity with the Cybersecurity Framework (CSF) and related documents.
https://www.nist.gov/cyberframework/framework

[4] The computer software and technology corporation (the software corporation) added, “One of the key benefits of the CSF is how it establishes a common language, which we use to facilitate security maturity conversations across our offerings in a consistent way. Consistency simplifies communications. It enables senior leaders to actively engage in discussions about security activities and continuous, repeatable improvements (e.g., making new investments in risk management processes/security capabilities).”

[5] Paging in this letter refers CSF version 1.1 with markup.
https://www.nist.gov/system/files/documents/2018/05/14/framework_v1.1_with_markup.pdf

[6] See Gartner glossary. Integrated risk management refers to “a set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks.”
https://www.gartner.com/en/glossary

[7] https://doi.org/10.6028/NIST.IR.7621r1

[8] https://www.nist.gov/privacy-framework
https://www.nist.gov/itl/ai-risk-management-framework

[9] According to the software corporation, “Many of the CSF’s subcategories [pp. 28–49] could be clarified. Our company develops subjectivity questions to support practitioners in understanding what the subcategories mean.” Further, the corporation noted, “Providing notional implementation examples along with the subcategories, similar to how the Secure Software Development Framework presents its contents, can better help practitioners make the connection between the subcategories and the tasks that they are familiar with.”

[10] https://www.nist.gov/news-events/news/2019/09/cybersecurity-framework-manufacturing-profile-low-impact-level-example

[11] https://csrc.nist.gov/projects/risk-management/about-rmf

[12] https://www.nist.gov/privacy-framework

[13] https://csrc.nist.gov/publications/detail/nistir/8286/final

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

[15] https://csrc.nist.gov/publications/detail/nistir/8259/final

[16] https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft

[17] https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework

[18] https://www.iso.org/news/ref2266.html

[19] https://www.iso.org/standard/72435.html

[20] https://www.federalregister.gov/documents/2020/03/20/2020-05823/navigation-and-vessel-inspection-circular-nvic-01-20-guidelines-for-addressing-cyber-risks-at

[21] https://www.itgovernance.co.uk/files/Infosec%20101v1.1.pdf

[22] https://csrc.nist.gov/projects/olir

[23] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[24] https://www.nist.gov/cybersecurity/improving-cybersecurity-supply-chains-nists-public-private-partnership

[25] https://www.federalregister.gov/executive-order/14028

[26] https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations

[27] https://www.ietf.org
https://www.ietf.org/id/draft-birkholz-scitt-architecture-00.html

[28] https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/publications

[29] https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft

[30] See the Chamber's April 10, 2017, letter to NIST on the "Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity."
https://www.nist.gov/system/files/documents/2017/04/20/2017-04-10_-_u.s._chamber_of_commerce.pdf

Also see some selected Chamber writings to NIST related to the CSF:

- February 7, 2018, "Primer on Chamber-NIST Cyber Collaboration."
https://www.nist.gov/system/files/documents/2018/02/01/2-7-18_vcat_matthew_eggers_chamber-nist_primer_final.pdf

- January 19, 2018, letter on "Cybersecurity Framework Version 1.1 Draft 2."
https://www.nist.gov/system/files/documents/2018/01/31/2018-01-19_-_u.s._chamber_of_commerce.pdf

- February 9, 2016, letter on "Views on the Framework for Improving Critical Infrastructure Cybersecurity."
https://www.nist.gov/system/files/documents/2017/02/13/20160209_us_chamber_of_commerce.pdf