CYBER RISK
INSTITUTE

April 25, 2022

Via electronic submission to CSF-SCRM-RFI@nist.gov

Attn: Katherine MacFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Dear Ms. MacFarland,

The Cyber Risk Institute (CRI)[1] appreciates the opportunity to provide comments to the National Institute of Standards and Technology's request for information incorporated within its Federal Register submission, *Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management.*

Attached, you will find CRI's submission. To develop it, CRI conferred with its member organizations and numerous other financial trade associations. Please do not hesitate to contact me if you have any questions or concerns.

Regards,

/s/

Joshua Magri
President
Cyber Risk Institute

[1] **About CRI:** The Cyber Risk Institute (CRI) is a not-for-profit coalition of financial institutions and trade associations. CRI is working to protect the global economy by enhancing cybersecurity and resiliency through assessment standardization. Its Cyber Profile – a freely available, freely downloadable tool – is the benchmark for cyber security and resiliency in the financial services industry. Learn more at https://cyberriskinstitute.org/.

CYBER RISK INSTITUTE

Cyber Risk Institute Response to the NIST CSF RFI

I. Summary

Thank you for the opportunity to comment on the National Institute for Standards and Technology's (NIST) Cybersecurity Framework Request for Information. The Cyber Risk Institute (CRI) is a not-for-profit association of financial institutions representing the broad diversity of the financial sector—from global institutions to community banks to cryptocurrency exchanges. CRI's mission is to provide a flexible framework based on leading practices to help the financial sector better manage cyber risk. This framework, the CRI Profile, is based on the NIST Cybersecurity Framework, used widely across the sector, and increasingly accepted by financial sector regulators. CRI looks forward to continuing to engage with NIST on ways to further improve the CSF's utility and applicability.

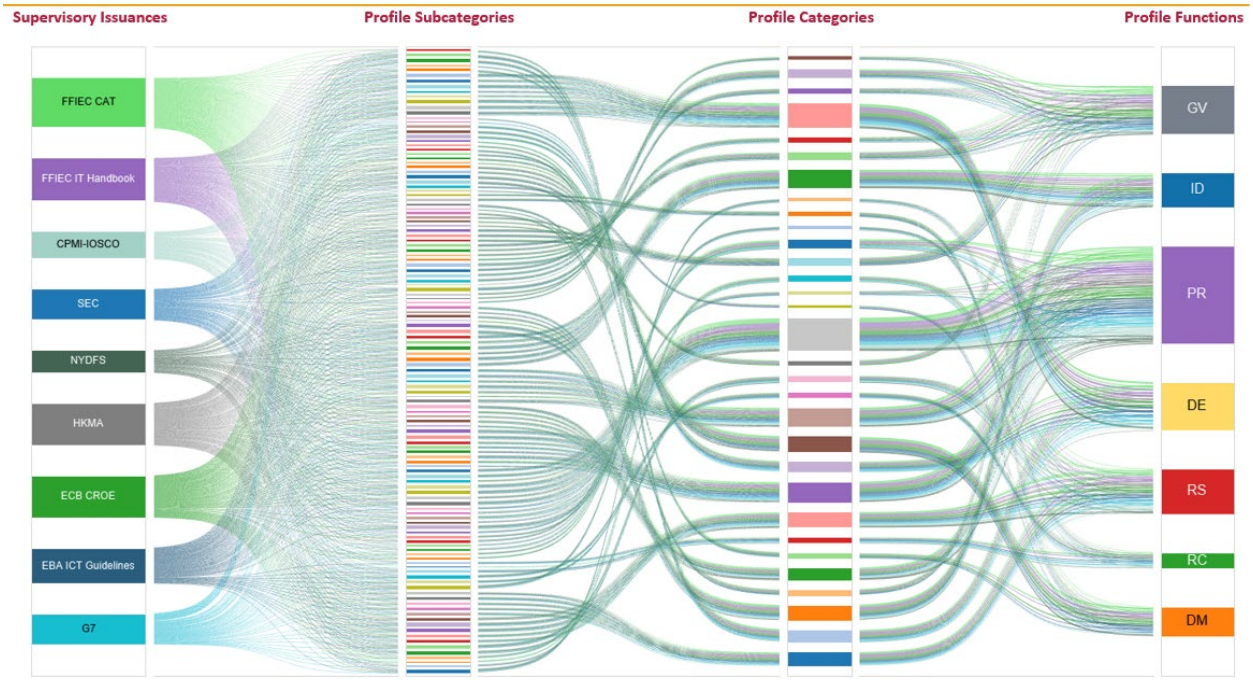
In summary, CRI recommends that any updates that NIST makes to the CSF should continue to utilize the Framework's architectural design simplicity, be incremental in scope, and that NIST undertake specific initiatives to make sure that the CSF's use is sustainable. **Keep it Simple. Incremental. Sustainable**. Accordingly, CRI offers the following recommendations, among other things –

- embrace the CSF's design as a topical "docking station";
- update the CSF to include the functions of "Governance" and "Supply Chain/Dependency Management";
- update the CSF to include other items, such as encryption and key management, secure software development, cloud computing and shared services models, new technology adoption and operational resiliency to reflect the changing cyber and technology risk landscape; and
- engage those agencies from across the globe that would be tasked with operationalizing cyber risk management for the industries they oversee.

II. The Cyber Risk Institute (CRI) and the Profile

A. Description of the Profile

The CRI Profile was developed by over 300 individual experts from over 150 financial institutions to help address growing financial regulatory expectations—and heightened fragmentation—related to cybersecurity. The Profile is based on the National Institute for Standards and Technology's (NIST) Cybersecurity Framework (CSF), but extended to include additional functions, control principles (called diagnostic statements), and regulatory references specific to the financial sector. This extension of the NIST CSF is a testament to the CSF's usefulness and broad applicability to the private sector. It is from this, in fact, that the Profile derives its name—it is a "Framework Profile" based on guidance provided in the CSF. It is also an indicator of how the private sector and organizations can elaborate on the foundational work NIST has accomplished to date. Like the CSF, the Profile is a framework for understanding cyber risk, and it has also been extended to be both a self-assessment tool and a means for institutions to communicate internally and externally. Figure 1 below depicts the supervisory issuances related to cybersecurity in the financial sector and how they align to the CRI Profile, and by extension, the NIST CSF.

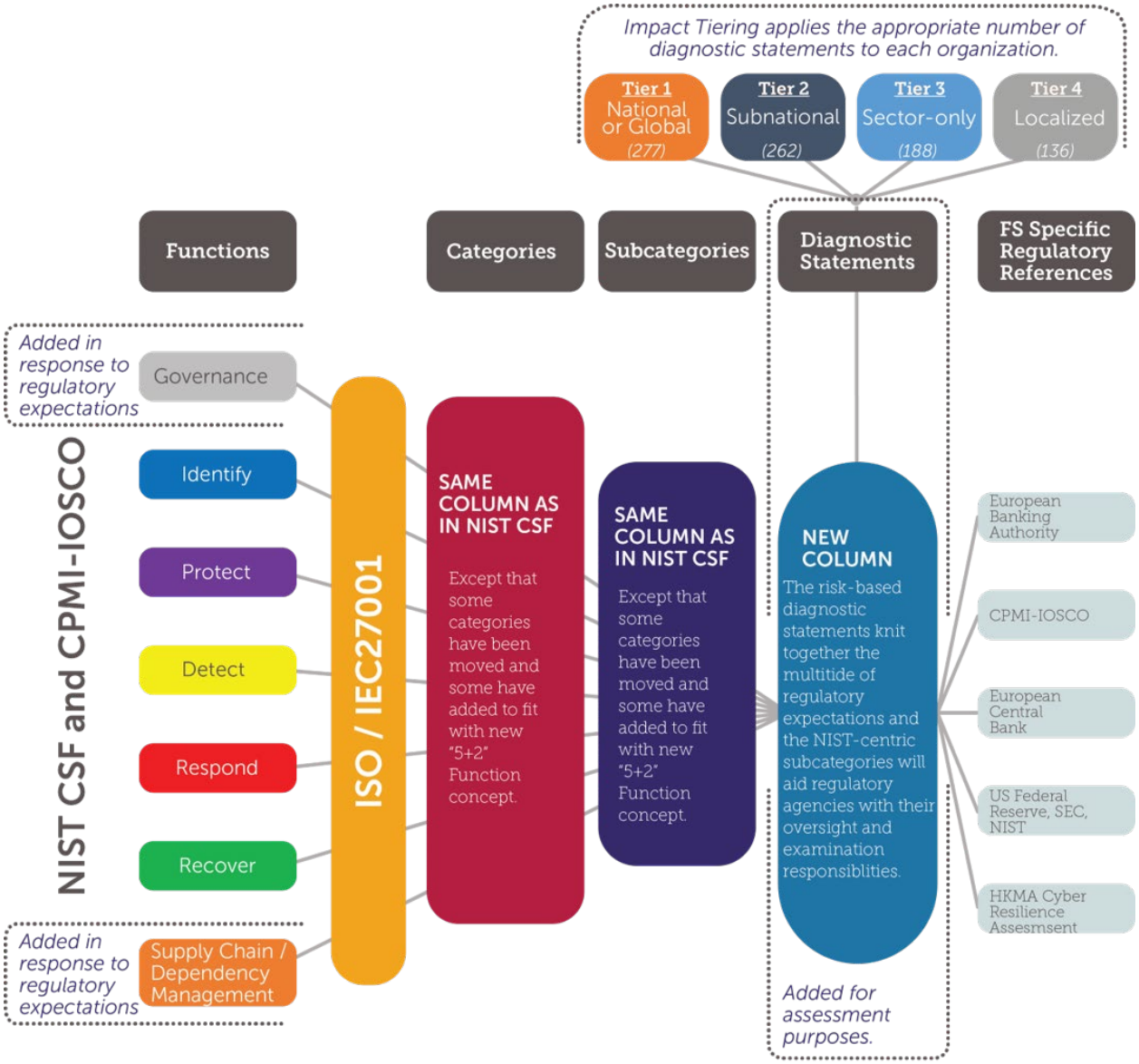


Source: Cyber Risk Institute

Specifically, the Profile includes a "Governance" function to address growing concerns related to cyber risk management and organizational alignment. This function includes categories from the NIST CSF's "Identify" function, such as business environment and risk management, as well as additional oversight and assurance activities. Additionally, the Profile includes a "Supply Chain/Dependency Management" function to address growing concerns related to third party risks faced by financial institutions and industry more broadly. This function includes categories from the NIST CSF's "Identify" function, such as supply chain and business environment activities. By elevating these control activities to a function, organizations are better able to communicate the critical elements of cyber risk management today.

Moreover, the Profile includes an "impact" questionnaire that allows an institution to adjust the number of controls it implements depending on its risk posture, in recognition that each organization has a different risk environment and tolerance. The impact questionnaire is based on global methodologies, such as the Basel Committee's determinations for globally systemic and important banks (G-SIBs), transaction volume, and interconnectedness. As a result, the Profile is usable for financial organizations of any size and can serve as a model for tailoring by other sectors. See Figure 2 for a description of how the financial sector extended the NIST CSF.

Figure 2: NIST CSF Extended for the Financial Services Sector



Source: Cyber Risk Institute

B. Private Sector Adoption of the NIST CSF

NIST stated that the CSF was intended to be a "*living document and will continue to be updated and improved as industry provides feedback on implementation.*"[2] The financial sector has been ahead of the curve in developing a NIST CSF-based Profile as an industry-specific assessment standard and risk communication tool. The NIST CSF continues to be the framework through which many financial services firms around the world are viewing and managing their cybersecurity risks. CRI currently has almost 40 members, which include institutions of all sizes, who endeavor to use the Profile internally

[2]National Institute for Standards and Technology, *Cybersecurity Framework version 1.1,* (Washington, D.C. April 16, 2018).

and externally. Additionally, one of CRI's key partners – the American Bankers Association – manages Profile peer groups, which collectively have over 300 participating institutions who regularly meet to discuss Profile implementation.

C. CRI Stands Ready to Assist

In 2018, the Financial Services Sector Coordinating Council (FSSCC) published version 1.0 of the Profile. Many of the same institutions participating in the Profile's development at that time established the Cyber Risk Institute as a vehicle to update and maintain the Profile. In 2020 and 2021, the Cyber Risk Institute published updates—versions 1.1 and 1.2—as well as a handbook that provided extended guidance on each diagnostic statement (i.e., control objective) and examples of evidence to support responses to those individual statements. In March 2022, CRI, in collaboration with the Cloud Security Alliance, published a cloud extension of its Profile: the CRI Cloud Profile.

From this work, CRI has accumulated a deep understanding of gaps in cybersecurity best practices and understands the challenge of ensuring that a framework is useful from both an organizational and practitioner perspective. Bringing this broad and practical experience, CRI is available and willing to assist NIST with future iterations on the CSF and ways to ensure that it remains applicable and flexible for organizations of varying sizes and complexities.

III. To Assure Continued Success, The Framework Must Continue to Utilize its Architectural Design Simplicity, Updates Must be Incremental in Scope and Its Use Must be Sustainable (Simple. Incremental. Sustainable)

A. Simple

The NIST Cybersecurity Framework (CSF) Should Continue to Utilize its Architectural Design Simplicity.

The NIST CSF's success and utility are largely due to its architectural design simplicity. Comprehensive (and complex) technical standards and jargon are synthesized into cyber security outcomes at the subcategory level, which are then further abstracted to the category level and a five-function level. These five functions—Identify, Protect, Detect, Respond, and Recover—are concepts that frontline defenders, executive leadership and the Board understand, and have enabled countless organizations to develop action plans around. CRI recommends that NIST maintain this core, with incremental additions, and follow the same discipline in its revision process, which has essentially allowed the CSF to be a modular "docking station" for current and future technology risk management concepts and topics.

Embrace the Docking Station Concept.

With the current CSF, the functions, categories, subcategories, and identifiers act as a classification system, enabling cyber security practices and other threat and security frameworks to "dock" to the CSF's activities and outcomes-based hierarchical groupings. This feature is why the CSF has at times been referred to as a Rosetta Stone, as it provides a means for practitioners across different disciplines (e.g., privacy, risk management, authentication, data loss prevention, and crisis response) to translate their practices into a commonly understood, simple, hierarchical taxonomy of activities and outcomes. CRI recommends that NIST maintain this design elegance as it considers CSF updates. New practices should be linked to existing activities and outcomes (i.e., existing categories,

subcategories, and functions) if they are or can be highly correlated.

Where, however, it is much more of a "correlative stretch," CRI recommends NIST develop a limited, synthesized set of new subcategories, categories, and functions that are the minimally disruptive to the overall NIST core/hierarchy while providing a credible "docking point" for the newly suggested items. This is what NIST did when it developed the *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0.* The Privacy Framework maintained the subcategory, category, and function structure, including the Identify and Protect functions, but it raised the governance activities (which had been in the NIST CSF's Identify function) to a new Govern Function (which is what CRI will be recommending in the Incremental Section of this document). It added two other Functions—Control and Communicate—because they were new concepts and would have been too much of a stretch to relate back to the other functions of the previously-published NIST CSF. In generating the table containing the Privacy Framework's core—the functions, categories, and subcategories—NIST highlighted where the Privacy Framework and Cybersecurity Framework shared the same functions, categories, and subcategories by highlighting those in gray. This approach has made use and implementation of the new materials easy and seamless.[3]

CRI recommends that NIST continue this "docking station" approach because this modularity will assure the CSF's broad applicability to organizations across all sectors and of different maturities. It additionally ensures its future adaptability to technology and risk management advances and the less-discussed, but just as important, shifting regulatory environment.

B. Incremental

NIST Should Update the CSF to Reflect Changing Landscape.

While the next version of the CSF should maintain its simplicity, it must also evolve to reflect the changing cyber and risk management landscape since the CSF was last updated in 2018. As more and more firms realize that cybersecurity is not just a technology issue, but an enterprise risk management issue, organizations, and those that regulate them, have appropriately increased their focus on internal organizational structures, as well as their internal and external (i.e., third party) policies and procedures. When developing the Profile, the sector recognized this trend within the financial services industry and modified its NIST-based "Profile" to expand and elevate NIST's Governance and Supply Chain categories to the function level—Governance and Supply Chain/Dependency Management, respectively—in the 2018 version 1.0 of the Profile.

While these additions were necessary in order to gain financial services regulatory community acceptance, these areas of focus are not unique to the financial services industry. Indeed, they are requisite for sound cyber risk management regardless of the industry. Telecommunications companies, like financial institutions, should have information security executives, who report regularly to the Board and who tie cyber security programs, policies, and processes to the firm's overall business objectives, risk appetite, and risk tolerance (i.e., Governance). Power companies should also understand their dependencies on third parties for delivering critical services, review those third parties' security and resilience programs, assess the availability of potential alternatives if

[3]This has not necessarily been the case with the release of NIST's other technical publications, which often lack explicit connectors and connection to the NIST CSF. CRI recommends that for future SP or NISTIR releases, NIST tie those back to the CSF in explicit and clear terms.

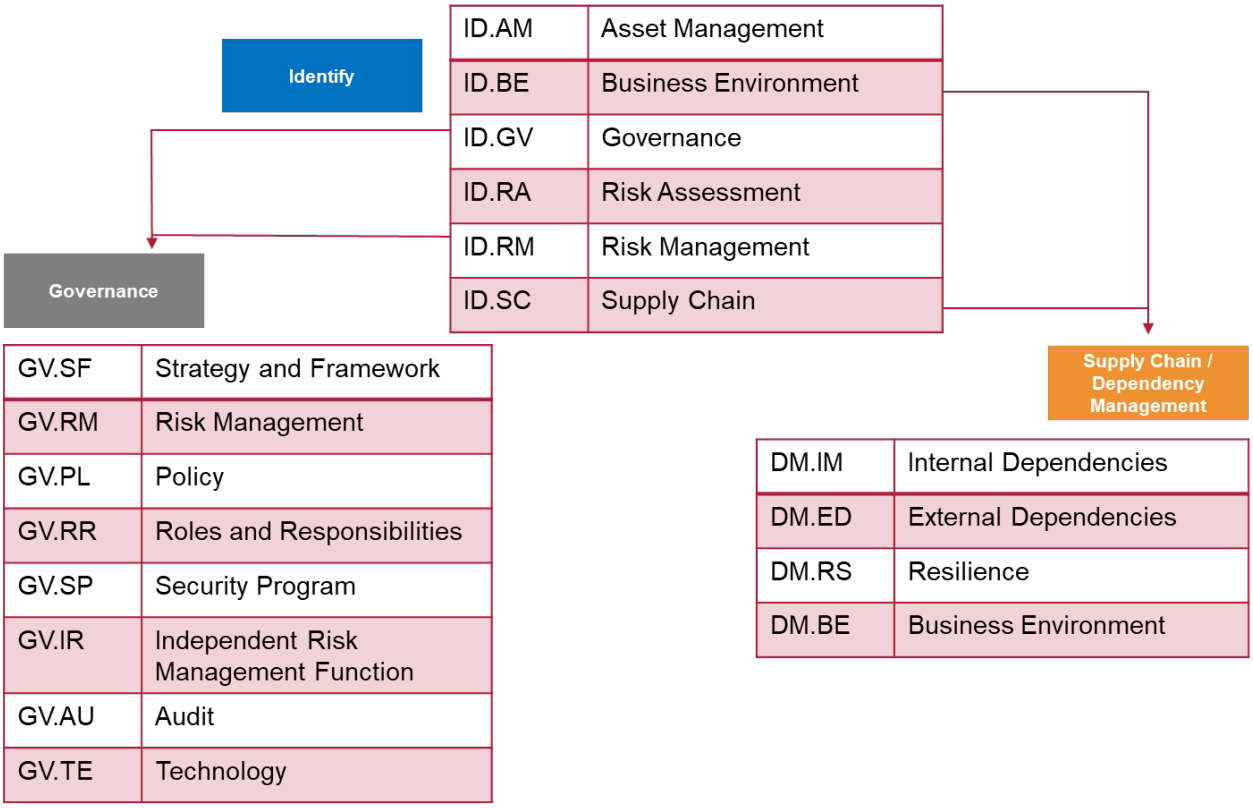
a key player is compromised, and determine whether the firm can provide critical services in a degraded state (i.e., Supply Chain/Dependency Management). As such, CRI recommends that NIST likewise elevate "Governance" and "Supply Chain/Dependency Management" to the function level in an updated CSF version 2.0.

NIST should elevate "Governance" to the function level, expand it to include risk management and governance categories from the "Identify" function, and further enhance it with additional risk management activities.

As mentioned previously, good governance is critical for cyber risk management, and it helps enable and ensure the success of an organization implementing the other critical functions and associated controls. Although the NIST CSF references some governance-related activities in its categories, and governance is discussed in the supporting CSF document's text, it is not called out specifically as a CSF function. NIST, however, has already taken an incremental step in elevating Governance via the Privacy Framework, wherein it established a "Govern" function, as is recommended here.

With respect to the Profile, CRI crafted the Governance function by incorporating the NIST CSF's risk management and governance categories taken from the Identify function, and further expanded upon them with additional considerations, such as policy-, audit-, and technology-related controls. Consequently, the Profile's Governance Function serves a "docking station" for controls related to organizational implementation of a cyber risk program, such as reporting to oversight bodies (e.g., the board of directors) and enterprise risk management. See Figure 3 for a description of how the CRI Profile's Governance function was developed.

Figure 3: Development of the CRI Profile's Governance Function



Source: Cyber Risk Institute

Moreover, although organizations find the CSF particularly useful in providing a framework for communicating with executive leadership and the board, it can be difficult for organizations to underscore the important role that oversight bodies and governance boards have on cybersecurity matters. The elevated visibility of an added Governance function will allow senior leaders to better appreciate their own responsibilities and reinforce the critical role they play in effective cybersecurity risk management. Additionally, governance crosses all domains of enterprise risk. Without effective governance practices, executive leadership may not know whether the underlying people, process, and technology controls could be poorly designed or not well aligned to business needs or objectives, thus introducing greater risk to the overall organization. Indeed, this is supported by Moody's recently released survey, *Cyber Risk – Global: Cyber risk survey of issuers finds growing investments, but gaps in preparedness*, in which it found "[s]ound cyber corporate governance practices determine the overall weight and attention an organization places on addressing cybersecurity risk."[4]

[4]Moody's, *Cyber Risk – Global: Cyber risk survey of issuers finds growing investments, but gaps in preparedness*, (New York: March 31, 2022). Attached, separately.

NIST should elevate supply chain to its own "Supply Chain/Dependency Management" function and augment it to include considerations on firms' internal and third party/supply chain dependencies, the firm's overall resilience, and the business environment in which they all operate.

From Solarwinds to Microsoft Exchange to Log4j, supply chain and third-party risks have been front and center all around the world, particularly as we have become increasingly interconnected and inter-dependent. Understandably, practitioners and overseers have been increasingly concerned with supply chain relationships and the roles and responsibilities of those who manage cyber risk management processes. To address these valid concerns, CRI recommends that NIST elevate supply chain as a CSF Function.

In its CSF adaption, CRI created a similar function—"Supply Chain/Dependency Management—in the Profile by incorporating the NIST CSF's business environment and supply chain categories from its Identify function. In the Profile, the Supply Chain/Dependency Management function was further enhanced by the addition of categories and subcategories related to management of these external dependencies and their impacts on operational resilience. In doing so, the Profile identifies where a firm should consider that it is dependent internally and externally for the delivery of critical services, how those services might continue when the firm or a supplier is operating in a degraded state, and oversight of the security practices of its third parties. Like the Governance function, the Profile's "Supply Chain/Dependency Management" function is designed to be modular and scalable, thus serving as a potential "docking station" for more detailed-level controls related to third-party and supply chain risk management.

Although effective cybersecurity supply chain risk management (C-SCRM) has been a key focus of the financial services industry for many years, it has risen to a level of national importance through President Biden's issuance of Executive Order 14028.[5] In response to that Executive Order, NIST published guidelines for identifying practices that enhance software supply chain security, among other things.[6] While NIST's guidelines reference using the CSF tier structure for organizations to baseline and measure their supply chain risk management programs, it also provides guidance for applying the NIST Risk Management Framework (RMF), a sound C-SCRM Practice Implementation Model, and suggestions for a C-SCRM Program Management Office and resourcing guidelines. Moving forward, NIST could make the linkage between this guidance and the CSF stronger and more explicit.

Indeed, NIST's C-SCRM Key Practices guidance could provide a sound basis for potential categories and subcategories for this newly proposed "Supply Chain/Dependency Management" function, in addition to the ones enumerated in CRI's Profile.[7]

---

[5]Executive Office of the President, *Improving the Nation's Cybersecurity,* (Washington, D.C.: May 12, 2021).

[6]NIST, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2nd Draft),* (Washington, D.C.: October 28, 2021).

[7]With this footnote, CRI is incorporating its Profile v1.2 by reference, which can be accessed at https://cyberriskinstitute.org/the-profile/, and recommends that NIST adopt CRI's function, category, and subcategory additions and augmentations.

NIST Should Consider Additional Areas for Incorporation and Linkage to the NIST CSF.

As mentioned previously, cybersecurity is no longer considered just an information technology issue, it is an enterprise risk management issue. As a result, organizations are increasingly looking for guidance and standards contextualizing cyber risk in more traditional business risk formats. Recently, NIST began publishing the NISTIR 8286 documents, which provide guidance on how organizations might contextualize cyber risk in business risk terms. As was done with the recent *Ransomware Risk Management: A Cybersecurity Framework Profile,* NIST should directly link the provisions in NISTIR 8286 with the NIST CSF (ideally, within the proposed, newly added Governance function), and expand upon the NIST CSF if needed, so that it provides an end-to-end playbook for time-strapped or less mature practitioners.

Other topics for considered integration and linkage to a new CSF include principles and practices are related to:

- encryption and key management;
- secure software development;
- cloud computing and shared services model;
- new technology adoption; and
- operational resiliency.

C. Sustainable

With architectural design simplicity and incremental changes to reflect the current threat, security, and regulatory environment, NIST can further assure the CSF's sustained and expanded use by simply making it easier to adapt.

CRI recommends that NIST make the CSF easier to adapt for implementation by:

- engaging those agencies from across the globe that would be tasked with operationalizing cyber risk management for the industries they oversee;
- providing guidance and templates on how the CSF can be extended in a consistent manner to meet technology-, industry-, or organization-specific cyber and regulatory needs;
- using OLIR and OSCAL to facilitate the integration of external best practices and standards, expository mappings and informative references; and
- maintaining an ongoing dialogue with CRI as it undertakes its own sector revisions to the Profile.

NIST should continue its promotion of the CSF globally and concentrate on more targeted solicitations of those agencies that would be tasked with operationalizing it for implementation within their industries.

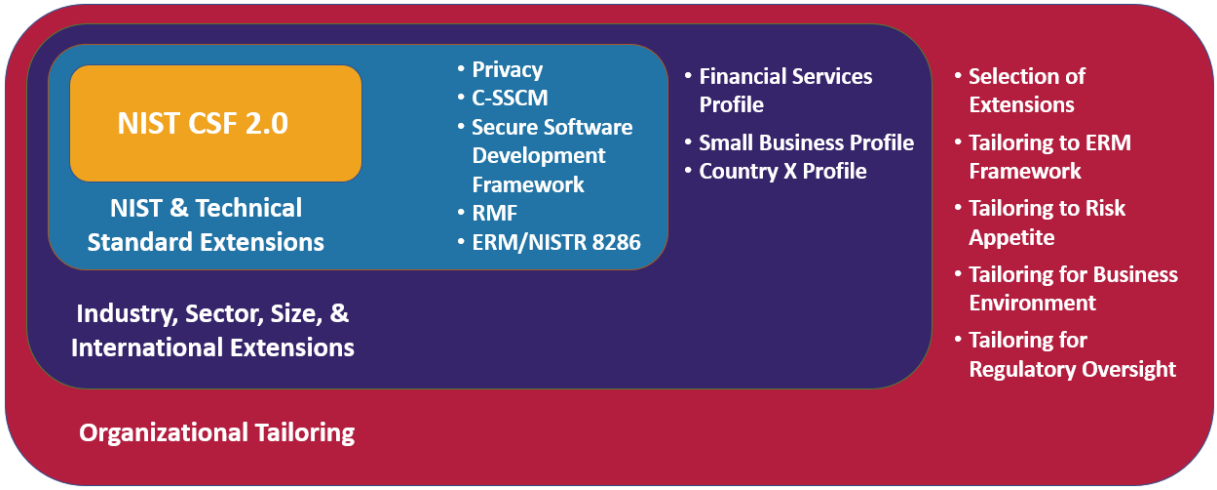
To expand and sustain the NIST CSF's use globally, it is important for NIST to engage the international community and integrate feedback in any update. While NIST has been successful in promoting the CSF at the national level in many countries, and in those countries' national cyber strategy documents, more work needs to be done. In particular, NIST should meet with sector-specific agencies and organizations that are responsible for translating national strategies into cyber regulation or cyber toolkits. Often, these agencies might be supportive of the NIST CSF concepts, but

do not necessarily know how to make it implementable within the industries that they oversee. NIST should be soliciting their feedback and devise corresponding templates and roadmaps to assist in the practical application of the CSF by and between those sector agencies and the private sector firms they oversee. Furthermore, the CSF itself, and those guidance documents, should be offered in those countries' native languages.

NIST should provide guidance on tailoring and extending the CSF.

In promoting the NIST CSF and the Profile, CRI frequently hears from organizations that they could use additional guidance on how to tailor and adapt the CSF (1) for a wide array of needs and (2) for sector-specific extensions, such as the CRI Profile, to easily integrate with an evolving ecosystem of regulations, standards, and frameworks. More specifically, we have heard that organizations are highly interested in receiving additional guidance and information on best practices related to implementing cybersecurity controls. See Figure 4 for how the NIST CSF core can be extended for various types of users and frameworks.

Figure 4: NIST CSF Sustainability through Extensions and Tailoring



To fulfill such requests, CRI has developed several techniques to facilitate the tailored implementation and use of the Profile, which could be used by NIST in providing guidance for tailored use of the NIST CSF. For example, the Profile's diagnostic statements provide additional levels of detail on subcategories and the Profile Workbook provides explanatory guidance on what diagnostic statements mean and what evidence is needed to support those statements. Similarly, the Profile created an industry-specific questionnaire to assign financial institutions to different tiers based on their potential critical infrastructure impact and tailors the controls by those tiers. Finally, CRI has developed "extensions" to the Profile to integrate it with other sound industry practices and provide tailored implementation guidance (e.g., with the Cloud Security Alliance's Cloud Controls Matrix (CCM)).

NIST itself created similar patterns for tailoring and extending the CSF in the Privacy Framework. In the Privacy Framework NIST replicated the same function, category, and subcategory structure as the CSF's; it included additional functions pertinent to the Privacy domain (e.g., "Govern"); and it

provided indicators of how the Privacy Framework categories and subcategories represent new, altered, or identical versions of the existing CSF categories and subcategories. The Privacy Framework also displays an "integrated" view of the Privacy and CSF Core structures meshed together to visually depict the intersection and extension of the CSF.

Organizations would find it helpful if NIST could provide patterns, templates, overlays, and, most importantly, guidance to assure consistent extensions and tailorings. For example, NIST could provide guidance on where and how a sector's regulatory provisions might architecturally fit in relation to NIST CSF subcategories. Additionally, NIST could provide a template for how various frameworks (e.g., MITRE ATT&CK or maturity methodologies (e.g., CMMI)) might "dock" into or overlay the CSF. As discussed with respect to the NIST Privacy Framework, NIST highlighted the interconnection between the later released Privacy Framework with the CSF through various illustrations and descriptions. This was highly effective and something that could be further expanded upon to drive consistency and future seamless use.

If NIST provided such guidance for how the CSF could be consistently extended and tailored, other sectors, individual organizations, and entire industries could be benefit in various ways. Such benefits might include ensuring that organizations consistently (1) integrate other subject matter domains that share a "Venn Diagram" intersection with cybersecurity, such as broader technology risk management, privacy, third party risk; (2) re-use framework component parts in these integrations, substantially easing adoption and increasing acceptance; (3) map to external regulations, standards, and frameworks; (4) tailor for targeted use by small- and medium-sized organizations; and (5) expand CSF visibility and adoption to reduce overall training required across their cybersecurity workforces.

NIST should use OLIR and OSCAL to expand integration of various mappings and informative references.

NIST's Online Informative References (OLIR) program can also play a significant role in the extension of the CSF's utility and useability. In aligning OLIR with the CSF extension framework described above, OLIR could become a key integration mechanism for external standards and frameworks and provide the "glue" to knit together the CSF and related extensions to mapped external standards, regulations, and frameworks

Similarly, NIST's Open Security Controls Assessment Language (OSCAL) program also could play a greater role in standardization and extension efforts. Moreover, numerous public, private, and non-profit organizations have been adopting, adapting, mapping, and using the NIST CSF over time. These organizations have deep knowledge that, if systematically captured, could help NIST more frequently iterate the CSF in targeted and sustainable ways, such as regular enhancements to informative references. While there are a number of informative references included in the NIST CSF, other candidates for inclusion exist and have evolved since the CSF's release. For a list of potential candidates for inclusion, please the Appendix.

NIST should continue to engage with CRI as it undertakes its own sector revision of the Profile to share in lessons learned.

CRI is in the process of making our fourth update and first substantial revision to the Profile, which will entail conducting a detailed gap analysis of the Profile against other financial services and technology industry regulations, guidelines, frameworks, and standards. CRI has mapped the Profile

to almost a dozen such frameworks and standards, including, for example, the FFIEC's Cybersecurity Assessment Tool (CAT) and the Cloud Security Alliance's Cloud Controls Matrix (CCM). Financial institutions have continued this work to map the Profile against NIST 800-53 rev. 4, COBIT 5, and other industry standard control frameworks.

CRI has consolidated these mappings into a single data source for the review and analysis of nearly 5,000 discrete comment and mapping entries (pairs of a Profile Diagnostic Statement mapped to a discrete source document statement/control objective). Approximately three-quarters of the mapping entries are designated as a "Full" mapping—meaning that there is strong correlation between the Profile and source document statement of requirement or objective. Although there is strong correlation between the Profile (and, by extension, the CSF) and other industry best practice standards and frameworks, gaps remain. CRI will be making selective changes to the Profile categories, subcategories, and diagnostic statements based on the gaps identified.

However, CRI's financial services members experience regulatory review and examination from a broader technology perspective, not just cybersecurity. As a result, the Profile may expand to include technology, operational resilience, and project management controls to acknowledge the relationship between cybersecurity and technology, and their roles in supporting organizational mission and risk management.

CRI recognizes that NIST will, of course, have other considerations in such scoping and inclusion/exclusion decisions, particularly as it balances the needs of various sectors and Federal agencies.

Just as we are recommending to NIST, CRI plans to be very judicious in making any change to the Profile and will pursue the principles of keep it simple, incremental, and sustainable. **CRI would welcome the opportunity to share its analyses, findings, and recommendations with NIST.**

Conclusion

We value the opportunity to provide detailed feedback on NIST's CSF and strongly support its revision by maintaining the guiding principles of keeping the CSF's architectural design simple, adding incremental amendments, and assuring sustainable use. CRI looks forward to participating in any other opportunities to provide feedback and assistance. On behalf of the Cyber Risk Institute and its members, we appreciate the opportunity to provide feedback on this important and timely update to the NIST CSF.

Appendix

To provide a more holistic Framework, NIST should consider the inclusion of the following standards as informative references if it should elect to expand the CSF to be more inclusive of technology and technology risk management related activities and outcomes:

1. The Information Security Forum Standard, aka "The Standard of Good Practice"
2. ITIL (The IT Infrastructure Library) v4
3. ISO 27004 - Information Security Management - Monitoring, Measurement, Analysis & Evaluation
4. ISO 27005 - Information Security Risk Management
5. ISO 27014 - Governance of Information Security
6. ISO 27033 - Network Security
7. ISO 27034 - Application Security
8. ISO 27035 - Security Incident Management
9. ISO 31000 - Risk Management - Guidelines
10. ISO 31010 - Risk Assessment Techniques
11. ISO 9001 - Quality Management
12. NIST SP800-30 - Guide for Conducting Risk Assessments (e.g., to ID.RA)
13. NIST SP800-39 - Managing Information Security Risk
14. NIST SP800-40 – Enterprise Patch Management
15. NIST SP800-55 – Performance Measurement for Info Security
16. NIST SP800-57 – Recommendation for Key Management
17. NIST SP800-83 – Guide to Malware Incident Handling and Prevention
18. NIST SP800-128 – Security-Focused Configuration Management
19. NIST SP800-144 – Guidelines on Security and Privacy in Public Cloud Computing
20. NIST SP800-160 – Systems Security Engineering
21. NIST SP800-161 – Supply Chain Risk Management