CYBER RISK INSTITUTE

CRI Response to NIST Concept Paper for CSF v2.0

March 2023

CYBER RISK INSTITUTE

March 17, 2023

To: National Institute for Standards and Technology

From: The Cyber Risk Institute

Subject: CRI Response to NIST Concept Paper for CSF v2.0

Thank you for the opportunity to comment on the National Institute of Standards and Technology's (NIST) *Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework*. We greatly appreciate the tremendous work NIST has completed to date in ensuring that the next version of the CSF is consensus-driven, internationally coordinated, and useful among organizations of all sizes.

The Cyber Risk Institute (CRI) is a not-for-profit association of financial institutions representing the broad diversity of the financial services sector—from global institutions to community banks to cryptocurrency exchanges. CRI's mission is to provide a flexible framework, called the CRI Profile, based on leading practices to help the financial sector better manage cyber risk. The Profile is based on the NIST Cybersecurity Framework (CSF), but extended to include additional functions, control principles (called diagnostic statements), and regulatory references specific to the financial services 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 NIST, in fact, that the Profile derives its name—it is a "Framework Profile" based on guidance provided in the CSF.

In our response to NIST's April 25, 2022, request for information on the Cybersecurity Framework (CSF), we recommended that NIST maintain its architectural simplicity of the CSF Core functions—Identify, Detect, Protect, Respond, Recover—and incrementally add two additional functions to help address critical elements of an organization's cybersecurity program—Governance and Supply Chain. We also recommended that NIST increase international engagement, develop sector-specific templates and guidance, expand the use of online informative references, and provide common standards to connect to relevant NIST frameworks. We are pleased that NIST's Concept Paper indicated that the agency would be incorporating many of these concepts in its development of the CSF version 2.0.

In our response below, we respond to a number of NIST's "Calls for Action," including providing detailed recommendations on how to build out a Govern function, a path forward on supply chain risk management, and suggestions for addressing measurement and assessment, among other things.[1] We hope to continue our engagement with NIST and fellow cybersecurity stakeholders to ensure that the future of the CSF is useable, extensible, and simple.

[1] In addition to the below, we suggest NIST consider how best to integrate the concept of "threat modelling" within the NIST CSF itself (potentially as a category or subcategory in the Identify function) and in related profiles.

Use the NIST-Based Financial Sector Cyber Profile as the Basis for Developing the Govern Function

CRI is pleased that NIST is including a new "Govern" function in the next version of the NIST CSF. The financial services sector and the regulatory agencies that oversee it have long valued sound cybersecurity principles. For example, regulators globally have been emphasizing the need for boards and senior leadership to grow their ownership of cyber risk management. Recognizing this importance, the CRI Profile includes a function on governance to reflect the important role that good, holistic governance plays in overall cybersecurity risk management. Elevating governance to its own function also indicates to boards and senior leadership that they play an important role in overseeing and managing cyber risk.

Based on our review of the CRI Profile and relevant NIST publications and frameworks—such as the Privacy Framework, ICT Risk Framework, and draft Artificial Intelligence Framework—there are several key governance-related considerations to properly manage various risk programs. These include organizations developing clear policies and procedures to manage risk, identifying roles and responsibilities, and conducting effective oversight. These all enable effective governance of programs whether they are cybersecurity, privacy, or emerging technologies.

As we examine cybersecurity specifically, we recommend that NIST review the CRI Profile's Governance function's categories and subcategories as a starting point for developing the CSF's Govern function, including:

- Strategy and Framework (GV.SF): The organization has a cyber risk management framework that is reviewed and approved by the Board and is informed by the organization's risk tolerances and its role in critical infrastructure.
- Risk Management (GV.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
- Policy (GV.PL): The organization has established a security policy in support of its cyber risk management framework.
- Roles and Responsibilities (GV.RR): The organization has designated appropriate roles and responsibilities, including an individual responsible for cybersecurity for the organization.
- Security Program (GV.SP): The organization has a cybersecurity program that is continually measured and improved.

Although the CRI Profile is made for and by the financial services sector, these categories and associated subcategories are relevant to any sector and examples of effective management of cybersecurity.[2] In fact, the CRI Profile's Governance (and Supply Chain) function(s) largely lift and shift categories and subcategories from the NIST CSF's Identify function. As such, these could be used as the basis for formulating NIST's Govern function.

Supply Chain Should Be Its Own CSF Function to Facilitate Ease of Use and Enhance Resilience

[2]The CRI Profile also includes three additional categories that are very important to the financial services sector and the three lines of defense model: Independent Risk Management Function, Audit, and Technology.

CRI strongly concurs with NIST's statement that supply chain risk management (commonly referred to as third-party risk management in the financial sector) issues should be expanded upon in the NIST CSF to a greater degree. As NIST notes in the Concept Paper, supply chain risk management often involves distinct assessment and oversight by separate teams or organizations. Based on feedback from our growing membership, this is clearly the case in financial services, especially as financial institutions have become increasingly reliant on third and fourth parties to conduct business operations. As a result, organizations would benefit from greater efficiency and clarity of processes, roles, and responsibilities should these cybersecurity-related outcomes be addressed more completely and distinctly in the next version of the CSF.

Moreover, organizations and regulators from around the world are increasingly focused on supply chain-related issues (e.g., the G7 "Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector" and the Prudential Regulation Authority's "Supervisory Statement – SS2/21: Outsourcing and third party risk management"). Elevating these outcomes demonstrates an understanding of the attention that supply chain risk management requires within organizations of all sizes and in all sectors. In today's environment, supply chain risk management is now clearly fundamental to sound cybersecurity risk management. CRI believes that the need to elevate the visibility of supply chain, or third-party, risk management is just as important as the need to elevate governance through a separate Govern function.

There are multiple ways in which these outcomes could be accomplished, which could include (but not be limited to): (1) establishing a new function, (2) distributing elements throughout the CSF under multiple functions, or (3) a combination of the two (i.e., a hybrid approach). CRI believes that a hybrid approach best allows cyber risk management outcomes that are inextricably linked with supply chain partners to be more concisely expressed. Based on our review of leading industry practices and regulatory issuances, the next version of the CRI Profile will take a hybrid approach that includes outcomes and control principles for important cybersecurity-related supply chain issues, particularly with respect to the life cycle management of third-party relationships. The governance of supply chain risk will be addressed in the Governance function. Specifically, the next version of the CRI Profile will likely include the following life-cycle third-party risk management categories:

- Procurement Planning: Documented plans are developed for procurements that involve elevated business, technical, or cybersecurity risk to the organization.
- Due Diligence and Supplier Selection: The organization performs thorough due diligence on prospective critical third parties, consistent with the procurement plan and commensurate with the level of risk, criticality, and complexity of each third-party relationship.
- Contracts & Agreements: Contracts clearly specify the rights and responsibilities of each party and establish protections to address the anticipated risks posed by a third party over the lifecycle of the relationship.
- Third-Party Management & Monitoring: Critical suppliers and partners are monitored to confirm that they have satisfied their obligations as required; reviews of audits, summaries of test results, or other equivalent assessments of suppliers and providers are conducted.
- Third-Party Relationship Termination: The organization anticipates, plans for, and executes third-party relationship terminations in a controlled manner.

For domain-specific objectives that involve coordination with third parties, such as recovery planning coordination, recovery plan testing, and incident coordination, will be included under the

CSF functions where they are currently addressed. Finally, software acquisition, integrity, and authenticity matters will be addressed in the systems development life cycle-related categories under "Protect". Regardless, NIST should actively consider how to incorporate/ integrate international standards in this fast-developing area to support the harmonization of standards.

CRI and Its Membership Volunteer to Contribute to the Development of Templates

CRI commends NIST for considering the development of guidance and templates to make it easier for organizations to adopt and implement the CSF. Because the CRI Profile is a template for sector-specific applications or extensions of the NIST CSF, CRI and our members offer to work directly with NIST to develop a template based on the Profile and for this to be used as the first template pilot implementation. This template could be used and adapted by other willing organizations or sectors. CRI has been approached by other organizations to describe the Profile's development, and its applicability and adaptability for other sectors.

NIST Should Consider Implementation Tiers and Measurement Next Steps

We agree with NIST that measurement and assessment of cybersecurity risk management is a critical issue with respect to use of the CSF. We also agree that there are many organizationally unique aspects of cybersecurity program implementation that require the use of different measures and metrics to adequately monitor and manage program outcomes. NIST's continued improvements to the *Performance Measurement Guide for Information Security* is a vital resource for organizations.[3]

In the area of cybersecurity program level assessment and program level maturity models, collecting and disseminating example implementations across organizations and sectors would certainly be helpful. However, we believe that NIST could play a much more significant and meaningful role in articulating the principles, characteristics, and attributes upon which sound assessment and maturity approaches could be predicated and developed. Despite the wide array of organizational implementations, we believe NIST could provide substantial value in proposing common means to assess program level effectiveness. While the challenges in developing such common principles are daunting, we believe this is an important area for NIST to provide thought leadership. CRI and our membership would welcome continued discussions with NIST and other sectors and organizations on such initiatives.

Success Stories Related to the NIST CSF

One of the key successes of the CSF, and by extension the CRI Profile, is the ability to adapt and expand coverage of other topic areas that are relevant to cybersecurity. CRI and its members are in the process of developing Profile version 2.0, which will include about 12 additional areas of cybersecurity and technology control programs, and expanded coverage of many other existing areas. For example, CRI will include greater coverage of encryption, key management, and forensics. We would be pleased to discuss these additional topics at NIST's convenience.

NIST CSF Extensions for Emerging Technologies and the CRI Cloud Profile as a Template

NIST states in its Concept Paper that it is reviewing the oversight of services related to certain emerging technologies, such as cloud security, while expanding the CSF's coverage of

[3]NIST, *Performance Measurement Guide for Information Security,* NIST SP 800-55.

governance and supply chain. It is crucial that the framework fully considers and integrates the potential impact of emerging technologies on key controls (e.g., 5G, Artificial Intelligence, Digital Assets, Quantum Computing) as those could have a significant impact on the control selection and ability for the framework to remain 'technology agnostic'. In particular, we encourage NIST to review the CRI Cloud Profile v1.2, which is an "extension" of the NIST CSF and CRI Profile by incorporating cloud implementation guidance, contractual responsibilities by service model, control types, and implementation phases.[4] Importantly, the Cloud Profile leverages the Cloud Security Alliance's Cloud Control Matrix and shared responsibilities nomenclature to create a mutual baseline of understanding between financial institutions and cloud service providers through the lens of the NIST CSF. CRI would be pleased to work with NIST to develop a cloud-specific CSF-based template that could be used by other willing organizations and sectors.

Leveraging Existing Frameworks for Secure Software Development

NIST invited feedback on the potential treatment of secure software development as part of C-SCRM outcomes. In 2020, BSA The Software Alliance issued an updated *The BSA Framework for Secure Software: A New Approach to Securing the Software Lifecycle*.[5] This framework is intended to assist with describing current and target states of software security, identifying opportunities for improvement in lifecycle management, and helping communicate and compare software security. BSA The Software Alliance also mapped version 1.1 of its framework to the NIST Secure Software Development Framework. We recommend that NIST consider incorporating elements from the BSA Framework for Secure Software into the CSF.

Conclusion

On behalf of the members of CRI, thank you for your consideration of these recommendations. We would be happy to discuss these priorities with you or answer any questions. We would also be pleased to further discuss the changes that will be included in the next version of the Profile, which CRI anticipates releasing this year.

Sincerely,

/s

Josh Magri
CRI President & Founder

[4] https://cyberriskinstitute.org/the-profile/
[5] BSA The Software Alliance, *The BSA Framework for Secure Software: A New Approach to Securing the Software Lifecycle,* (September 2020; Washington, D.C.). https://www.bsa.org/files/reports/bsa_framework_secure_software_update_2020.pdf