BOSTON CONSULTING GROUP

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

From: The Boston Consulting Group

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

Date: April 25, 2022

Dear Ms. MacFarland,

The Boston Consulting Group is pleased to submit this response to National Institute of Standards and Technology (NIST) Request for Information (RFI) on Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management. Our response to this RFI focuses on NIST Cybersecurity Framework.

Based on our experience, BCG believes NIST Cybersecurity Framework has been tremendously valuable for the business community by providing a clear way to organize, manage, aggregate, and report cybersecurity activities. By doing so, the Framework helps communicate cyber risks to broad audiences including boards and executives. We very much appreciate the opportunity to contribute to the future Framework revision and look forward to the evolution of the Framework.

Any questions about the content of this response can be directed to Nadya Bartol at Bartol.nadya@bcg.com or +1 301-922-9537.

Sincerely,

Nadya Bartol
Managing Director
BCG Platinion

BOSTON CONSULTING GROUP

Error! Reference source not found.

1.1 Use of the NIST Cybersecurity Framework

1. ***The usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions in the Framework and actively managing risks using those five functions.***

   NIST Cybersecurity Framework has become the de facto standard for many organizations all over the world, of all sizes, scopes, and complexities. Our client organizations find NIST Cybersecurity Framework Functions, Categories, and Subcategories extremely helpful for organizing, managing, aggregating, and reporting their cybersecurity program activities. Our clients find the ability to roll up information from Subcategories to Categories to Functions especially useful in summarizing the state of cybersecurity and communicating it to non-technology executives and the Boards as the Framework provides an easily accessible way to explain the state of cybersecurity in non-technical terms. We also find that less mature and/or smaller organizations can use the Functions, Categories, and Subcategories to define the minimum set of activities and then expand and grow their cybersecurity programs in a structured way.

2. ***Current benefits of using the NIST Cybersecurity Framework.***

   a. ***Are communications improved within and between organizations and entities (*** **e.g.,** ***supply chain partners, customers, or insurers)?***

      Yes, NIST Cybersecurity framework has been immensely useful as far as providing a frame of reference and lexicon for describing cybersecurity functions, capabilities, and processes. Our client organizations often seek to benchmark themselves relative to peer organizations using the NIST CSF as a basis for that comparison.

   b. ***Does the Framework allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks?***

      Yes, the NIST Cybersecurity Framework is useful for effective risk management in a few dimensions. First, it serves as a basis for organizations to conceptualize the different layers/or dimensions of risk mitigation available (e.g., Identify, Protect, Detect, Respond, Recover). Second, it provides organizations with a basic understanding of the different activities necessary for risk management via the subcategories captured in the 'Identify' function.

   c. ***What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?***

      We believe that metrics should be based on goals and objectives and should capture relevant activities. As such, NIST SP 800-55 rev1 provides the appropriate processes and structured to capture metrics relevant to NIST CSF Functions, Categories, and Subcategories. Additionally, our clients find it helpful to measure their NIST CSF maturity to understand the current state of their cybersecurity

programs, establish a target state, and then conduct regular check ins and assessments to measure progress towards the target state.

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

While many organizations have adopted the Framework, there is still confusion as to which cybersecurity framework to use (e.g., NIST CSF, NIST SP 800-53, CIS Top 20, FFIEC CAT, ISO/IEC 27001, etc.). Organizations still at times use different frameworks for different purposes which increases compliance burdens without a lot of value for cybersecurity improvement. This confusion may be caused by the particular preferences of cybersecurity leadership, regulatory compliance, geographic location, or simple lack of awareness caused by insufficiently experienced workforce.

Additionally, organizations early in their cybersecurity journey or those facing resource constraints may find it difficult to perform all of the cybersecurity activities described within the NIST CSF. These organizations may be left overwhelmed and wondering where to begin. While it is possible for organizations to combine NIST CSF with other guidance such as CIS Critical Security Controls, this is challenging to accomplish and frequently requires specialized support that not all organizations are able to acquire and afford.

4. ***Any features of the NIST Cybersecurity Framework that should be changed, added, or removed. These might 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 Cybersecurity Framework; or references to critical infrastructure versus the Framework's broader use.***

As NIST notes in this RFI, much has changed since the initial publication of the Framework in 2014 and it's update in 2018 to include the threat, regulations, and technology environment. Additionally, numerous other frameworks have been published and updated that have expanded and extended what the NIST Cybersecurity Framework provides. We believe that the following topics could be expanded and enhanced in the future revision of the Framework:

- **Governance** – governance and executive leadership support has become a key cybersecurity topic. From experience working with clients in multiple industries we know that without appropriate governance structures and executive leadership support organizations are limited in their ability to activate and maintain the right programs that would appropriately manage cybersecurity risks. It should be noted that there are two frameworks already in existence that have a Governance function: NIST Privacy Framework and Cybersecurity Risk Institute Profile. We believe that Governance should be broken out into a separate function which would absorb and expand the Categories and subcategories from Identify including ID.BE, ID.GV and ID.RM.

BOSTON CONSULTING GROUP

Error! Reference source not found.

- **Supply Chain** – Managing cyber risks from supply chains is another area that has become paramount to protecting the enterprise. Notably, the Cyber Risk Institute Profile includes a Supply Chain/Dependency Management Function that constitutes an expanded ID.SC CSF Function. Supply chain is another area to consider for breaking out into a separate function that should be further aligned with already existing NIST guidance on the topic including NIST SP 800-161 and the SSDF.

- **Security in SDLC/ Designing Security In** – The NIST Framework addresses cybersecurity for an operational organization and has minimal amount of content dedicated to developing secure software. Many organizations that use the Framework have substantial SW Development groups and are faced with adding another framework (e.g., SSDF or BSIMM) to cover all their related activities. Furthermore, developing secure software is paramount for improving global and national cybersecurity postures because that is how weaknesses and vulnerabilities get into our digital environments, including through the supply chain. Adding a Category that addresses Security in SDLC (or Designing Security In) within the Protect Function, aligned to existing NIST guidance to include the SSDF, would help organizations have a set of practices available within the NIST Framework and address evolving software supply chain challenges.

- Performance Measurement and Metrics – While supporting guidance specifically mentions metrics and measures, the NIST CSF itself only goes as far as to allude to them. Organizations find it very difficult to manage what they do not measure, and therefore there is an opportunity to emphasize the importance of metrics and measures (e.g., Key Risk Indicators (KRI), Key Performance Indicators (KPI), or Objectives and Key Results (OKR)) in a more pronounced manner within the Framework itself. When combined with data analytics and risk quantification capabilities, metrics and measurers can significantly improve the quality and accuracy of information available to decision makers within the organization. Adding a Category to specifically address activities necessary to source, synthesize, monitor and report, and continuously improve metrics and measures would help move organizations to data-driven decision making and supplement the effectiveness of existing risk management guidance. We suggest adding this Category to the above suggested Governance function with specific Subcategories to provide organizations the right level of guidance.

- Risk quantification – There is an opportunity to emphasize the importance of quantitative methods for risk analysis (e.g., as done in NISTIR 8286 series). The availability of tooling and training to support these methods has substantially grown over the past 10 years, making these methods more accessible to a larger set of organizations. Additionally, quantitative risk analysis and accompanying techniques (e.g., expert estimation) are empirically shown to outperform traditionally qualitative methods for risk analysis by improving accuracy and reducing bias. (Anthony (Tony) Cox Jr. – What's Wrong with Risk Matrices, Douglas Hubbard, Richard Seiersen – "How to Measure Anything in Cybersecurity Risk"). Organizations would benefit from guidance on how to use these methods (e.g., to inform cyber investment decisions) and what the key activities might be for effectively implementing this capability. We realize that lower maturity organizations will find this a challenging

activity. Our suggestion is that risk quantification could be mentioned as an appropriate evolution to include in risk assessment methodology under ID.RA, among other potential methodologies..

- Resilience - the current Framework does not include mention of Resilience, which exists as the intersection between Incident Response, Business Continuity Management (BCM), and Disaster Recovery. Business Continuity Management in particular is limited to PR.IP-9 in the current version of NIST CSF. Evolving threats that organizations face (e.g., ransomware) reinforces the importance of effective organizational resilience capabilities. There is an opportunity to elevate the resilience topic including the different dimensions of BCM within a NIST CSF category (e.g., Identify). Specifically organizations need to understand activities required to achieve resilience, such as business impact analysis that identifies maximum allowable downtime (MAD), recovery point objectives (RPO) and recovery time objectives (RTO) which are foundational for any business continuity or disaster recovery capability.

- Enterprise integration of cyber risk management– throughout the framework there is an opportunity to emphasize that effective cyber risk management is integrated with the enterprise-level risk management. Examples of specific areas where enterprise integration could be emphasized include supply chain risk management (with procurement, enterprise risk management (ERM), risk strategy & assessment (with ERM). Doing so would follow in the spirit of other NIST publications (e.g., NISTIR 8286 series which emphasizes the importance of integrating cybersecurity and ERM). This could be achieved by an addition of a subcategory or changing the language under ID.RM or, as we hope NIST would consider, GV.RM.

- Cryptography, Encryption, and key management – There is an opportunity to emphasize the importance of encryption, key management, and cryptography related activities. These activities are critical to an organizations ability to effectively protect sensitive information. Given the complexity of these activities, this guidance is all the more important. This could be achieved by adding one or more subcategories under PR.DS.

- Threat Intelligence - While threat identification is emphasized in the current Framework, there is an opportunity to consolidate and expand guidance (e.g., into an identify category) related to the holistic set of activities that drive effective threat intelligence capabilities (e.g., collection, processing, analysis, dissemination). Threat intelligence activities are important for understanding current environment and ensuring the right response and warrant an additional Category under Identify with specific Subcategories to provide organizations the right level of guidance.

5. ***Impact to the usability and backward compatibility of the NIST Cybersecurity Framework if the structure of the framework such as Functions, Categories, Subcategories, etc. is modified or changed.***

BOSTON CONSULTING GROUP

Error! Reference source not found.

We believe that useability and backward compatibility are important, but the world and the practice have changed substantially. We would advise NIST to keep the structure the same, fill in the gaps that the community identifies, but keep constant those parts of the framework that can be kept constant.

6. Additional ways in which NIST could improve the Cybersecurity Framework, or make it more useful.

We believe there is an opportunity to improve the usability of the NIST CSF in a few dimensions:

- **Prioritization of CSF Activities (e.g., subcategories).** While we acknowledge that there is no one-size-fits all solution to prioritization of cybersecurity activities, we do believe that the community at large would benefit from a general perspective on which capabilities should be prioritized when building a cybersecurity capability within an organization. Even a simple, 3-tier framework would help organizations discern foundational activities from those that are performed by more advanced, well-resourced organizations. This would add usability to the framework for organizations of all sizes and state of capability.

- **Interdependency of CSF activities (e.g., subcategories).** In almost every instance, one cybersecurity activity is dependent on the outputs of another activity to deliver a holistically efficacious outcome (e.g., asset management informs risk assessment and vulnerability management). We would advise NIST to capture the interdependencies among the different activities within the NIST CSF. As organizations implement the expansive set of activities described within the NIST CSF, they would benefit from a readily available view of those dependencies to inform their resource allocation. This would be particularly useful to organizations as they make cybersecurity strategy and roadmap decisions. This would make the Framework more usable for organizations of all sizes and state of capability. This recommendation would build on the outputs of the recommendation to prioritize CSF activities.

- **Creating a CSF Maturity Model**. While the NIST CSF implementation tiers are a significant first step, there is a real opportunity to define a maturity model based on the NIST CSF. We recognize and acknowledge the immense undertaking of this activity. However, at present, organizations rely on private interpretations of maturity across different activities described within the NIST CSF. Use of maturity models has become ubiquitous among organizations. These maturity models aid organizations in communicating their progress implementing cybersecurity programs to internal and external stakeholders. Adopting a consensus-based maturity model would facilitate planning and information sharing among organizations and benefit the community at large. Given the size and complexity of this undertaking, creating a separate guidance document, rather than adding a maturity model to the CSF may be appropriate.

Error! Reference source not found.

Error! Reference source not found.

1.2 Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources

7. ***Suggestions for improving alignment or integration of the Cybersecurity Framework 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 Cybersecurity Framework. These resources include****:*

   - *Risk management resources such as the NIST Risk Management Framework, the NIST Privacy Framework, and Integrating Cybersecurity and Enterprise Risk Management (NISTIR 8286).*
   - *Trustworthy technology resources such as the NIST Secure Software Development Framework, the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline, and the Guide to Industrial Control System Cybersecurity.*
   - *Workforce management resources such as the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity.*

   NIST provides tremendously helpful resources to the global community. However, these resources are often difficult to consume and use due to them being published in PDF documents. Moving these resources into an environment that would dynamically link the resources and allow online access to multiple resources would help improve usability of these resources and knowledge for the individuals using them.

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

   Unfortunately, since the publication of the NIST Framework the multiplicity of non-US frameworks and approaches, as well as of regulations, has increased exponentially. Since each of these frameworks, approaches, and regulations has a specific purpose and audience, there are numerous commonalities and inconsistencies at the same time. Solutions to alignment are in faster updates, greater collaboration, dynamic analyses and access, as well as work by all in the community to reduce the number of resources that the practitioner has to consume and understand.

   Additionally, it would be greatly appreciated if NIST updated the informative references to include the most recent NIST SP 800-53 Rev5, ISO/IEC 27002:2022, CIS Top 20, COBIT 2019, and IEC 62443-2-4:2015.

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

   In our experience NIST CSF is already one of the two prevalent global frameworks being used by companies throughout the world, the second framework being ISO/IEC 27001 and/or ISO/IEC 27002. Additionally, a series of ISO/IEC JTC1 SC27 standards already exist, that do their best to align NIST CSF with ISO/IEC 27000 family of standards. Namely, ISO/IEC 27100, ISO/IEC 27110, and ISO/IEC 27013. Continued efforts to educate global audiences on the existence of these standards, as well as how they and ISO/IEC 27000 family of standards align may be helpful in reducing the clutter of continuously increasing cybersecurity regulations, as well as increasing international adoption of NIST CSF.

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

    We very much welcome this initiative to provide a reference catalog to numerous standards, guidelines, frameworks, etc. proliferating throughout the world. We believe that at a minimum ISO/IEC JTC1 SC27 family and IEC 62443 series of standards should be referenced in this resource. Other documents that should be referenced include industry-specific versions of NIST CSF, such as Cyber Risk Institute Profile, and authoritative industry guidelines, such as Cloud Controls Matrix by Cloud Security Alliance.