ITI Promoting Innovation Worldwide

April 25, 2022

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

Via email to: CSF-SCRM-RFI@nist.gov

RE: ITI Response to National Institute of Standards and Technology (NIST) Request for Information on Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Dear Ms. MacFarland:

The Information Technology Industry Council (ITI) appreciates the opportunity to respond to the National Institute of Standards and Technology's Request for Information (RFI) on *Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management*. ITI is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, and related industries.

Cybersecurity and cybersecurity technology are critical to ITI members. Facilitating the protection of our customers (including governments, businesses, and consumers), securing and protecting the privacy of individuals' data, and making our intellectual property, technology, and innovation available to our customers to enable them to improve their businesses are core drivers for our companies. Consequently, ITI has been a leading voice in advocating effective approaches to cybersecurity, both domestically and globally. Cybersecurity is rightly a priority for governments and our industry, and we share a common goal of improving cybersecurity. Further, our members are global companies, doing business in countries around the world. Most service the global market via complex supply chains in which products are developed, made, and assembled in multiple countries around the world, servicing customers that typically span the full range of global industry sectors, such as banking and energy. We thus acutely understand the impact of governments' policies on security innovation and the need for U.S.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

policies to be compatible with – and drive – global norms, as well as the potential impacts on our customers.

As both producers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy. In the technology industry, as well as banking, energy, and other global sectors, when discussing any cybersecurity policy, it is important to consider our connectedness, which is truly global and borderless.

ITI has been engaged in NIST's Framework efforts for the better part of a decade, working to provide constructive input and shape the Framework to make it as useful as possible, and appreciate the opportunity to provide additional feedback as NIST considers if and how to further revise the Framework. We continue to see the Framework provide immense value to users, within critical infrastructure but also beyond. That said, there has also been a significant amount of government activity aimed at improving cybersecurity and addressing risks, particularly with the issuance of the *Executive Order on Improving the Nation's Cybersecurity* (Executive Order 14028). Although supply chain cybersecurity was considered to some extent in version 1.1 of the Framework, it has taken on increased prominence, especially in the context of software supply chain security. As such, we appreciate that NIST is asking stakeholders important questions about ways in which integrating supply chain security can increase the overall effectiveness of the Framework.

We organize our responses based on the themes NIST has laid out in the RFI, focusing first on use of the NIST Cybersecurity Framework, then on the relationship of the Framework to other resources, and finally offering perspectives on if and how NIST should address supply chain in the Framework.

Use of the CSF

As a general matter, we believe that the Framework has been a highly useful tool for cybersecurity risk management, offering a baseline approach for organizations seeking to institute such a process. Indeed, to the extent the goal of the Framework was to provide a common language for organizations, it has certainly achieved that, proving useful for communicating about cyber risk both within and between organizations. This is one of the major benefits of using the Framework. Mapping to consensus standards and control sets helps to provide a common, international understanding of the intention of the categories and sub-categories, and the Implementation Tiers provide a reference point for organizations to evolve their ability to cybersecurity programs.

The Framework has also provided for a risk-based, flexible approach, allowing organizations to develop a cyber risk management program that is appropriate for their level of risk, desired outcomes etc. – the flexibility that comes with using the Framework is key to improving cybersecurity. It is also worth mentioning that the Framework is used by organizations beyond

critical infrastructure owners/operators, demonstrating the utility and applicability of the Framework beyond its original target audience.

At the same time, there are challenges that organizations face when using the Framework. For example, there remain very real resource constraints, particularly for small and medium size businesses. Additionally, there remains within some organizations a lack of personnel with the skills and/or knowledge needed to digest, understand, and apply the Framework. Additionally, organizations may face competing priorities when choosing whether and how to implement the Framework, which can make it difficult to utilize it easily and robustly.

Another challenge in using the Framework is around benchmarking and understanding how an organization is doing in practically implementing the Framework. Although Version 1.1 helpfully added a section on self-assessment, including around how measurement can serve to improve cybersecurity risk management practices, members noted that the Tiers remain somewhat vague and so it can be difficult to understand how to utilize them. It is also not clear to some organizations how to measure the effectiveness of particular controls, and some of our members wondered whether it would be possible to determine which sets of controls actually result in fewer cyber incidents. There is also a lack of robust guidance in the current Framework around the Profiles and how to use them, including to explain how and when an organization should determine its current Tiers across Core practices or how it should develop a Current and Target profile.

Beyond that, some of our members noted that sometimes organizations view the Framework as more of a compliance tool than it was intended to be, for instance by using it to value their overall level of security instead of leveraging it as a risk management starting point. Using the Framework in this way could lead to a sense of complacency for organizations who believe that so long as they are achieving the outcomes that are laid out in the CSF, they are secure. One of the reasons for this is that for many, NIST 800-53 was an overwhelming document, so when the CSF was published, organizations leveraged it as a replacement, without really understanding that the intended use of the Framework is to implement it via leveraging Informative References such as 800-53. Although we appreciate that NIST attempts to clarify this in Version 1.1 of the Framework, specifically stating that the core functions should *not* be used as a checklist of actions to perform, we offer some additional suggestions that we believe would help to address this issue and some of the other challenges noted above.

Recommendations

Consider ways to make the Framework's outcomes more objective. In the current version of the Framework, the outcomes are rather subjective, resulting in inconsistent interpretations and confusion around how to implement various categories or subcategories to achieve said outcomes. In order to achieve this:

- ***NIST should seek to strengthen the Profiles section of the Framework.*** Additional information about the purpose of the Current and Target Profiles would be useful,

including guidance on how an organization can assess what its target state should be. Indeed, developing both Current and Target Profiles does not necessarily enable an organization to manage their cyber risk portfolio. Step 2 of Section 3.2, "Orient" states that "the organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets," but no additional information is provided as to how to conduct or integrate this threat/vulnerability assessment into the Framework. Given this aspect of the Framework is critical to improved risk management, we encourage NIST to add additional detail on how this orientation should be conducted, and how that should be integrated into both a Current and Target Profile. It may also be useful to incorporate guidance around *when* the Target Profile should be developed. Although developing a Target Profile early on could be helpful to determining where there might be gaps in an organization's cyber risk management process, developing such a Target Profile too early may also mean an organization lacks useful context that may be derived from a Tiers-based assessment.

- ***NIST should strengthen guidance around Tiers*.** We also encourage NIST to further build out guidance related to the Tiers. As referenced above, the Tiers are currently vague and challenging for many organizations to interpret. In our prior comments on CSF Version 1.1, we suggested that NIST develop a methodology that organizations could use to assess what Tier they might fall into, and we reiterate here that additional substantive information on each Tier, in addition to developing a methodology, would be helpful so that organizations can determine where they might be. It might also be useful to consider adding guidance around how an organization can achieve each Tier.
- ***NIST should consider ways to improve guidance for organizations about how to meet expectations for some of the subcategories.*** This might include tasks that at a minimum an organization should perform to meet the subcategory, given some of the subcategories are extremely large in scope (e.g., identity and access management). In the alternative, if subcategories are not modified to incorporate the concept of expectations, we suggest considering how to improve the usefulness of the informative references by perhaps splitting them into two categories to guide implementers: NIST authoritative references (with definitive mappings into NIST 800-53/82) and non-NIST informative references (mappings into other frameworks and authorities). Since there is no context provided except the references themselves, we understand that implementers are getting confused and both viewing and using them as authoritative (complete references that outline the controls that need to be implemented in order to meet the subcategory).
- ***NIST should further consider how to address challenges around measuring the effectiveness of Framework implementation.*** In its Version 1.1. update, NIST helpfully included a new section on self-assessment. Although a step in the right direction, we believe that additional information is required so that organizations can understand how their implementation of the outcomes associated with the Framework Core might compare with implementations by other, similar organizations. One way NIST might be able to address this is to consider if and how to provide anonymized benchmarking, or other anonymized case studies, so that organizations can more objectively assess where they stand compared to other similarly-situated organizations.

Seek to carry forth foundational principles of flexibility and adaptability that the original Framework was based in. The foundational principles on which the Framework was based remain relevant. We encourage NIST to keep these principles in mind as it seeks to update the Framework. Indeed, one of the key reasons the Framework has been so widely adopted, even outside of critical infrastructure sectors, has been because it can be used with a broad array of cyber risk management processes by a diverse group of stakeholders. It avoids being too prescriptive but provides helpful references for organizations seeking to implement the functions and categories they have determined are commensurate to their risk appetites. Flexibility and adaptability should continue to be a foundational consideration guiding the development of Version 2.0 of the Framework.

Consider whether adding an explicit Governance function would be useful. As we referenced above, we believe that the five functions offer a robust way in which entities can organize their cybersecurity risk management processes. However, we note that in both the *Privacy Framework* and the *AI Risk Management Framework: Initial Draft*, NIST includes a stand-alone Governance function, with categories/subcategories focused on cultivating a culture of risk management across the organization. Although we believe the original five functions are a useful construct and understand that Governance is already incorporated within the existing Identify function as a category, we encourage NIST to further consider the role that Governance plays in cybersecurity risk management and whether such a stand-alone function might also be worth incorporating into the CSF, given the role that an organization's culture can play in risk management more broadly. Doing so may additionally make sense given that one of NIST's express purposes in contemplating this update is to consider how the CSF interrelates and aligns with other Frameworks; it might be worth considering whether adding a separate Governance function to CSF could help illuminate how it relates to and aligns with the Privacy and AI Frameworks.

Relationship of the NIST CSF to other Risk Management Resources

We appreciate the immense amount of work that NIST has undertaken in developing risk management resources, as well as its commitment to engaging with stakeholders throughout the process of developing these resources. That being said, there are now a plethora of NIST resources which can sometimes be confusing to organizations, particularly as they seek to determine if and how to leverage them. Above, we referenced several challenges related to use of the Framework, but the relationship of the Framework to other NIST resources is another important point to keep in mind as NIST considers how to update the Framework.

In particular, since the last Framework update, relevant items that NIST has published include the Secure Software Development Framework (SSDF), an Initial Draft of the AI Risk Management Framework, the Privacy Framework, and an update to 800-161, among others. Although useful, it can be difficult to understand if and how these various guidance documents overlap, if at all, and how they can be integrated into an organization's overarching risk management process.

Recommendations

Consider developing additional crosswalks to other frameworks. NIST created a helpful crosswalk between the Cybersecurity and Privacy Frameworks, which is useful for organizations in understanding where the Frameworks overlap and which functions and/or categories and subcategories apply. A high-level mapping similar to that which exists in the Privacy Framework, as well as a more detailed one akin to the one posted here, would both be helpful, particularly for documents like the AI RMF and the SSDF.

More specifically consider how secure software development practices interrelate with the Framework. We encourage NIST to consider how secure software development practices relate to the Framework. The importance of and need for a greater focus on software assurance has increased, as evidenced by the central role of secure software development in Section 4 of Executive Order 14028. While we applaud NIST for the development of the *Secure Software Development Framework*, we believe NIST's update to the Framework provides an important opportunity to make clear how the SSDF should interact and be used with the Framework, and how and where secure software development practices may be applicable within the Framework itself. It might be helpful for NIST to develop a crosswalk or conduct a mapping exercise between the Framework and the SSDF so that organizations can better understand how the two interrelate.

Consider exploring the relationship between the Framework and existing certification programs. While the Framework is not and should not be construed as a certification program, it might be worthwhile to explore how the Framework relates to existing certification programs, including which categories might be applicable to prominent certifications. For example, if an organization has a SOC2 or is FedRAMP certified, how and where do those various certification requirements map to the Framework? Organizations might find such a mapping between the Framework and the certifications illuminating.

Add some of the more technical documents produced by NIST beyond 800-53 to informative references where appropriate. In revising the Framework, we encourage NIST to add to and/or update the Informative References. While we recognize that the Informative References are intended to be illustrative and not exhaustive, we believe it would be helpful to add several additional references. For example, mapping NIST 800-37, FIPS 140-3, NIST 800-63 and NIST 800-213 may be useful. While 800-161 is also critical to supply chain risk management, seeking to integrate and/or map 800-161 in its entirety would likely make the Framework unwieldly. However, there may be key practices in 800-161 that are relevant to an organization's overall cybersecurity risk management process that could be highlighted. We explore considerations around supply chain security risk management in the context of the Framework in the "Supply Chain" section below.

Encourage harmonization of federal cyber initiatives and agency guidance with the Framework to increase use of the Framework. As NIST is well-aware given its prominent role in many federal cybersecurity efforts, there is a significant amount of activity occurring across the

federal government aimed at improving cybersecurity, particularly as a result of Executive Order 14028. The establishment of the Office of the National Cyber Director (NCD), which was in part created to help establish federal coherence on cybersecurity strategy, offers a unique opportunity to drive harmonized approaches. We encourage NIST to work with the NCD to manage agency use of the Framework more proactively, as required per *Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Indeed, we believe that the Framework, if appropriately supported across the USG, could help to unify federal cyber efforts, acting as a baseline for federal agencies.

We also note that pursuant to the *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems*, NIST, in conjunction with CISA, released a set of preliminary cybersecurity performance goals, in part to facilitate more tangible implementation of the outcomes associated with the Framework. We also understand that NIST and CISA are now working to develop sector-specific cybersecurity performance goals.[1] While at a minimum the performance goals should be aligned with the Framework, we encourage NIST to consider if and how the performance goals might be integrated into the Framework. For example, can they be mapped to subcategories as Informative References?

Continue to map international standards to the Framework to further encourage alignment, undertaking periodic reviews to update the international standards that are already included as informative references. Although we recognize that it is difficult to update the Framework every time a new international standard is completed, we encourage NIST to undertake a periodic review and update the Informative References as appropriate. As efforts to develop the 2.0 version of the Framework get underway, it seems like an appropriate time to review and update the many international standards incorporated in the Informative References. For example, we recommend that the Framework align with and reference the new ISO/IEC 27110 Cybersecurity Framework Development Guidelines, which was initially started based on the NIST Cybersecurity Framework, but which has been further updated and adapted via the international standards consensus process to be applicable internationally.

Continue international engagement and outreach on the Framework. International engagement will be imperative to continue advancing efforts to improve cybersecurity globally and support a consistent approach to cybersecurity risk management. NIST should continue to participate in cyber dialogues led by the Department of State, commercial dialogues and other efforts led by the International Trade Administration, and in multilateral fora like APEC on cybersecurity and related topics to build upon its already robust international engagement efforts. Capacity-building and training around the use of the Framework will also remain key to implementation, so we urge NIST to consider how it might continue to support those sorts of efforts.

[1] See NSM here: https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

We also stress the importance of promoting international adoption through international standards bodies such as ISO/IEC. There is a long history of regional or country specific standards bodies such as NIST submitting their standards to an international forum such as ISO/IEC as the foundation of new standards. Such standards are then adapted and adjusted via the international community to be globally applicable. Many international governments are concerned with adopting country-specific standards and/or Frameworks; however, they understand the quality and value of these standards, and once brought through an international forum where they have the opportunity to contribute, are more likely to leverage them.

Supply Chain

We appreciate that NIST has launched the National Initiative for Improving Cybersecurity in Supply Chains (NIICS) effort, and that it is considering how to more robustly integrate C-SCRM into the Framework. C-SCRM has only increased in importance since the 2018 update, including with the proliferation of additional guidance documents, and we believe it is a useful endeavor to think about how to address it in the context of the Framework.

Recommendations

Ensure that NIICS efforts are harmonized with other ongoing supply chain efforts. This is a perennial ITI recommendation, but we think it is once again worth emphasizing. There is a glut of government policymaking activity focused on supply chain security and it is oftentimes not clear how such policies fit together. By way of illustration, the Information and Communications Technology Supply Chain Risk Management (ICT SCRM) Task Force resources library catalogues over 20 supply chain-related efforts taking place across the Federal Government, and that list continues to grow. While we recognize that the NIICS is less of a policy-focused effort, it is still important that it is aligned with and/or that NIST makes clear how it fits with these ongoing efforts. Additionally, other groups are undertaking work in areas that may be implicated under the NIICS that may be relevant to the conversation (see, e.g., the ongoing SBOM work being led by CISA, efforts under the ICT SCRM Task Force, etc.) There is a need to ensure complementarity between the new NIICS effort and other ongoing activities aimed at improving cyber supply chain risk management. Overall, we believe that NIICS, with robust stakeholder engagement and input, will provide an opportunity to rationalize and streamline the myriad supply chain security efforts.

Consider that there are both benefits and potential drawbacks to more robustly including C-SCRM into the Framework. There are likely both benefits to incorporating C-SCRM considerations more robustly into the Framework, as well as benefits to covering C-SCRM separately. For example, including some of the newer C-SCRM resources in the informative references might be an appropriate way to further integrate C-SCRM into the current iteration of the framework. NIST could also include further narrative at the outset around the resources that have been developed recently and an explanation of how they relate to and should be used in conjunction with the Framework. It also may make sense to integrate C-SCRM more

fully by including categories throughout the functions, as opposed to only under the Identify function.

On the other hand, there has been *a lot* of recent activity on C-SCRM, especially resources produced by NIST and because of that, the Framework could be overwhelmed by C-SCRM guidance if NIST seeks to incorporate *everything*. Additionally, the audiences for C-SCRM and Framework implementation may differ and integrating significant C-SCRM guidance may serve to engender confusion. At the same time, because there are so many Frameworks already, adding another, separate one focused solely on C-SCRM is likely not an ideal solution, as it could add more complexity to an already saturated landscape. So, we recommend against developing an entirely separate C-SCRM Framework.

Instead, NIST should seek to include C-SCRM references in the Framework, potentially by adding categories to every subfunction, but aim to limit the amount of information included to that needed by cybersecurity risk managers to better enable overall risk management. There may, however, be value in establishing guidance as to how an organization can use the Framework to improve supply chain cybersecurity, perhaps as a separate Profile.

NIST should consider developing guidance for organizations around engaging with and contributing to open-source communities. Another increasing area of focus is the secure development of open-source software and the potential risks that might stem from the use of open-source software. Many open-source projects will not incentivize or require the use of the SSDF, CSF, or other practices stemming from EO 14028. However, we believe that NIST providing guidance in this area may be helpful so that organizations who do not engage deeply with open source and government consumers of open-source projects can be made aware of compensating controls that might be adopted relative to the use of open-source in certain contexts and have an understanding of other risk management strategies that may be appropriate to undertake.

***

As long-time advocates on behalf of the Framework and partners to NIST in developing versions 1.0 and 1.1, we appreciate the opportunity to engage with NIST as it considers updates to create Version 2.0. The Framework has proved a highly successful tool over the years since its inception that has positively impacted the cybersecurity of thousands of organizations, and we are appreciative that NIST is thinking about how to continue to improve the resource and promote additional uptake. We look forward to continuing to collaborate with NIST as it goes through the process of updating the Framework to create Version 2.0. Please reach out with any questions.

Sincerely,

John S. Miller
Senior Vice President of Policy
and General Counsel

Courtney Lang
Senior Director of Policy