ITI Promoting Innovation Worldwide

November 4, 2023

Via email to: cyberframework@nist.gov

Re: ITI Response to National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 Draft and Implementation Examples

The Information Technology Industry Council (ITI) appreciates the opportunity to provide feedback on the National Institute of Standards and Technology's *Cybersecurity Framework 2.0 Draft and Implementation Examples (CSF 2.0 Draft).* 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.

We have been engaged throughout NIST's process to update the Cybersecurity Framework, submitting comments to the initial Request for Information, the Concept Paper, and the Discussion Draft focused on the Core. When the Concept Paper was released, we were happy with the direction that the changes were taking at that point and were also glad that nearly all of our comments were reflected in technical changes to the Discussion Draft of the Core. After reviewing the full CSF 2.0 Draft, we have limited feedback given the CSF 2.0 draft once again incorporated nearly all of our suggested edits. We are especially pleased with the way in which supply chain risk management has been integrated throughout the six functions. We offer a few additional suggestions below on the Govern function, Supply Chain sections, and Implementation Examples but are on the whole supportive of the way NIST has adjusted the CSF 2.0 Draft and developed Implementation Examples.

Govern

We continue to support the new Govern function, which has been aligned with our overarching suggestion that NIST focus on governance in the update of the CSF. We believe the addition of this function will improve cybersecurity risk management across organizations and will also make the Framework easier to use with the other NIST Frameworks. The narrative does an excellent job explaining the purpose of the Govern function and also delineating which part of the organization should be responsible for setting the overarching risk management strategy and how that cascades down to the business process and operational levels. We appreciate that the narrative also discusses the intersection of the Privacy and Cyber Frameworks, and that it includes some references to the AI Risk Management Framework (AI RMF).

However, we continue to believe that further discussion of the areas in the AI RMF that may overlap or otherwise intersect with the Cyber Framework would be helpful to

Global Headquarters [redacted]
Europe Office [redacted]
info@itic.org
www.itic.org
@iti_techtweets

highlight. For example, Appendix B of the AI RMF explains how AI risks are different from traditional software risks, but also explains how both privacy and cybersecurity risk management considerations are applicable throughout the design, development, deployment, evaluation, and use of AI systems. Specifically, the AI RMF highlights that two of the trustworthiness characteristics proposed under the AI RMF – Secure and Resilient and Privacy-Enhanced – intersect with both the Privacy and Cyber Frameworks. While we recognize that AI is a specific technology in a way that 'cyber' and 'privacy' are not, we think it would be useful to include further discussion of this intersection where the narrative points to the AI RMF, particularly because it may not be readily apparent where there are commonalities between all three Frameworks and how an organization leveraging AI may already be applying (or how it could be applying) controls that are referenced in not only the Cyber and Privacy Frameworks, but also the Secure Software Development Framework (SSDF).

Supply Chain, First-Party, and Third-Party Risk

We have also been supportive of NIST's efforts to integrate cyber supply chain risk management into the CSF more holistically, including in categories throughout the functions, because in practice C-SCRM is something that should be integrated across an organization's risk management processes. We are generally supportive of including Supply Chain in the Govern function to indicate outcomes an organization should consider in creating a cyber supply chain risk management program and also appreciate that NIST has added language identifying exemplar categories in other sections that may pertain to C-SCRM. However, it may be useful for NIST to consider specifically highlighting additional categories under these other Functions in the Core itself that may be relevant to supply chain risk management under different functions; for example, Roles & Responsibilities under Govern (GV.RR) and the Awareness and Training Category under Protect (PR.AT), Continuous Monitoring under Detect (DE.CM). We previously recommended this and reiterate that recommendation here.

While we recognize it has been challenging to determine how best to holistically incorporate C-SCRM into the CSF, we continue to believe it would be helpful to delineate and identify where categories under other functions beyond the specific Supply Chain category under Govern implicate or otherwise address supply chain risk. As we had highlighted in our prior comments, although sophisticated organizations may intuitively understand which sections address supply chain-related risks, many smaller organizations may lack such awareness, potentially leading to confusion as they endeavor to develop their own C-SCRM programs as part of their overall cybersecurity risk management strategies. If it is not possible to somehow flag the C-SCRM relevant sections within the text of the Core itself – one way might be to simply include parenthetical text indicating which categories are relevant to C-SCRM –perhaps another way might be to include this information in a standalone section such as an appendix.

We also previously offered several additional suggestions regarding third- vs. first-party risk throughout the Core. We appreciate that NIST has more clearly delineated in certain subcategories third-party risk considerations, but we wonder whether there might be an

opportunity to more clearly describe how the first- and third-party risks differ. As we recommended in our prior comments, we think there is a way in which NIST could highlight the first vs. third-party risks throughout the categories and subcategories – both those that are explicitly identified as SCRM as well as those that are not explicitly SCRM but may have a SCRM-component. Although several of the Implementation Examples discuss this to some extent (e.g. GV.SC-06, ID.AM-04), we continue to believe that a more granular indication of first-party, third-party, and other supplier-related risks throughout the Core will be useful. As we discussed above, if it is not feasible to somehow include this information directly in the Core, an appendix could be a place where NIST could more specifically highlight these differences.

One of the primary and long-term benefits of the CSF is that it has created a common language, which helps organizations better manage and communicate cybersecurity risks. But, if first-party and third-party supply chain risk are not identified and explained effectively in the Core, NIST runs the risk of creating more confusion around C-SCRM and making it more difficult for users, especially first-time users, to manage these risks.

Additionally, we believe there is also opportunity for NIST to discuss the shared responsibility model in greater depth in the narrative portion of the Draft CSF 2.0. There is one bullet under 3.4.2, Improving Communication with External Stakeholders that states "define shared responsibility models with cloud service providers," but we believe that more content is needed here. One bullet does not provide sufficient guidance to the many organizations of all sizes utilizing cloud services who are seeking to leverage the framework. Additional detail about what the shared responsibility model means in the context of supply chain risk management would be useful information to add.

Additionally, although we did not highlight this in our prior comments, upon further discussion with members we suggest that NIST consider revising the language specific to Continuous Monitoring under the Detect function -- specifically DE.CM 06, which suggests that external service provider activities and services are monitored to find potentially adverse events. The term 'monitoring' has raised some concern in that in certain cases, undertaking a 'monitoring' activity implicates disclosure and/or notice requirements in some states and localities. Changing this to read as 'oversee' would address this issue.

Implementation Examples

We are supportive of NIST's decision to include Implementation Examples as a part of the updated Cybersecurity Framework. We think this will be instrumental to organizations seeking to understand concrete actions they could take in order to operationalize the outcomes associated with each function.

We had previously suggested that NIST include narrative language clearly indicating that the examples are not exhaustive or prescriptive, and further, that many other implementation examples are possible. We reiterate that previous recommendation. It would also be helpful to note that not all implementation examples are necessarily relevant to all organizations and risk profiles.

We think this is particularly important in order to preserve the nature and intent of the CSF – a principles-based, flexible Framework that organizations can adapt based on their risk tolerance and goals. Focusing on *what* organizations should do to manage cybersecurity risk, and not prescribing *how*, remains especially important in light of an increasing government appetite for greater business accountability in mitigating cybersecurity risk through governance and oversight processes. We understand that the Implementation Examples are not intended to be prescriptive, and that the CSF is not intended to be regulatory in nature, but it sets a high bar for proactive steps that organizations can take to manage cybersecurity risk. Adding narrative language that indicates the Implementation Examples should *not* be interpreted as prescriptive contracting (or other) requirements in the future would be useful. While we understand that NIST has decided to host the Implementation Examples separately from the CSF itself in order to allow for more flexibility in updating them, we worry that this will detract from the CSF 2.0 being understood as a single Framework and may result in the Implementation Examples being understood and used as a guide for *how* the CSF may be implemented. If NIST maintains the decision to separately list Implementation Examples, we strongly encourage NIST to prominently display language somewhere at the top of the landing page so that when organizations (or the government) search for relevant Implementation Examples they understand their intended purpose and context immediately.

We have one specific recommendation for the DE.CM Implementation Examples that related to our suggestion above regarding the language around Continuous Monitoring in DE.CM 06. We suggest changing the word 'monitor' to 'oversee' in the Implementation Examples as well.