ITI Promoting Innovation Worldwide

June 9, 2023

ITI Response to National Institute of Standards and Technology (NIST) Discussion Draft of the Cybersecurity Framework 2.0 Core

The Information Technology Industry Council (ITI) appreciates the opportunity to provide a response to the National Institute of Standards and Technology's Discussion Draft of the *NIST Cybersecurity Framework 2.0 Core.* 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, following on our sustained engagement during the processes that produced the 1.0 and 1.1 versions of the Framework, including submitting comments to the initial Request for Information as well as the Concept Paper. As we indicated at the time, we were supportive of the direction that the changes were taking when the Concept Paper was released, and we continue to be supportive of the direction of the changes as outlined in the discussion draft of the Core. However, while we were pleased to see that nearly all of our high-level comments are reflected in the draft changes to the Core, we believe that certain of the technical changes could be more effectively implemented.

Below we offer overarching thoughts on how to further improve the Core:

Govern

One of the significant proposed changes that was introduced in the Concept Paper, and which is now incorporated in the Core, is the inclusion of a new Govern function, which is aligned with our prior suggestion that NIST add a sixth function focused on Governance. With the inclusion of the Govern function, not only does the Framework now better align with NIST's *Artificial Intelligence Risk Management Framework (AI RMF)* and *Privacy Framework*, but importantly the Govern categories and subcategories accurately reflect practices that organizations can and are already undertaking to create a culture of cybersecurity across business units. We also positively note that many of the categories in the new Govern function align with those included in the Privacy Framework.

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

However, while not a major concern, we question whether the Awareness and Training category that exists under the current Protect function would also be better suited to sit under the Govern function, as it does in the Privacy Framework. To some extent it is covered as a subcategory under Roles and Responsibilities, but it may be useful to include it under Govern to further emphasize the important role that Training and Awareness plays in fostering a culture of cybersecurity risk management across an organization. Further, we continue to maintain it would be helpful for NIST to include a graphic visualization depicting the relationship of the Govern function to the existing functions in its first draft of the Cyber Framework 2.0, such as that exists in the AI RMF.

Supply Chain Risk Management and Third-Party Risk

In our response to both the RFI and the Concept Paper, we recommended that NIST integrate cyber supply chain risk management (C-SCRM) more holistically into the Framework, including in categories throughout the functions. Our rationale was that C-SCRM is something that should be integrated holistically across an organization's cybersecurity risk management processes and approaching incorporation of such practices in a holistic way supports such an approach. However, our overall assessment of the changes to how C-SCRM is addressed in the draft Core is that to the extent there was an effort to integrate the topic more holistically, it falls short, for several reasons.

First, while in certain cases, such as within the Govern function, NIST has added categories that were previously housed under the Identify function focused on C-SCRM, we note that the bulk of the categories and subcategories that are explicitly labeled as relating to supply chain continue to be maintained in a single Supply Chain category under Identify. Retaining this macro-level structure is slightly misleading insofar as it inadvertently signals to CSF users that SCRM is primarily a Govern-related issue rather than a more holistic organization-wide risk management issue.

Second, there are other areas of the Core which clearly deal with supply chain related risks, but which are not explicitly called out as such (e.g., in the Roles and Responsibilities category of Govern (GV.RR) and the Awareness and Training category under Protect (PR.AT)). While sophisticated organizations may intuitively understand these sections as also addressing 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. We recommend that NIST more clearly identify these categories as also dealing with aspects of supply chain risk management. Doing so could also help alleviate the first issue identified above.

Third, we believe NIST could more effectively delineate the differences between first-party and third-party risks throughout the SCRM-related categories and subcategories (both those that are explicitly identified as SCRM – including in the SCRM category that is a part of the Govern function – and the various other places throughout the Core that address first-party, third-party and supplier-related risks, including as noted above). While we note that some of this important nuance is addressed in the first "implementation example" (ID.RA-01), we encourage NIST to consider taking a more granular and nuanced approach when referring to first-party, third-party and supplier-related risks throughout the Core. One of the enduring benefits of the CSF has been that it created a common language to help organizations better manage and communicate cybersecurity risks; lumping together first-party and third-party supply chain risks as reflected in the draft Core 2.0 may increase confusion around C-SCRM and make it harder for some stakeholders to effectively utilize the Framework to manage third-party supply chain risks and other dependencies.

Implementation Examples

We are supportive of NIST's decision to include Implementation Examples as a part of the updated Cybersecurity Framework, as including this section will be instrumental to organizations seeking to understand concrete actions they could take in order to operationalize the outcomes associated with each function. In terms of level of abstraction, we think the examples as drafted are sufficient, although we encourage NIST to build out further examples. Additionally, we encourage NIST to include prefatory language in this section to make clear that the list of examples is not intended to be exhaustive or prescriptive. Specifically, NIST should make it abundantly clear to Framework users that many other implementation examples are possible, that not all implementation examples are necessarily relevant to all organizations and risk profiles, and discourage the use of the implementation examples as a compliance "checklist." Finally, we think the format suggested by NIST in which an additional column lists the Implementation Examples is appropriate.

* * *

In closing, ITI would like to thank NIST for its continued leadership and partnership in developing the Cybersecurity Framework 2.0. We look forward to continuing to work with you as you work toward finalizing the document and are happy to answer any questions you may have regarding our comments.