January 19, 2018

Edwin Games
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Via e-mail to: cyberframework@nist.gov

RE: ITI comments in response to NIST Request for Comment - "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 Draft 2."

Dear Mr. Games:

The Information Technology Industry Council (ITI) appreciates the opportunity to respond to the National Institute of Standards and Technology's (NIST's) request for comment of December 5, 2017, seeking feedback on the *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 Draft 2* (hereinafter, "Draft 2").[1]

ITI, the global voice of the tech sector, is the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry, and represents leading companies from across the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, and Internet companies. ITI has long commended NIST's work in partnering with the private sector and other stakeholders to further the development and use of the voluntary *Framework for Improving Critical Infrastructure Cybersecurity* (the "Framework"), and Draft 2 incorporates important changes to deepen and broaden the effectiveness of the Framework in helping a broad array of stakeholders better manage cybersecurity risks. ITI continues to support the approach embodied in the Framework, which leverages public-private partnerships, is grounded in sound risk management principles, and helps foster innovation due to its flexibility and basis in global standards.

We are pleased to see that Draft 2 reflected several of the recommendations ITI offered to improve the first draft of Version 1.1,[2] including: (1) changes to the new section on cybersecurity measurement and metrics to emphasize the role of measurement as a tool for self-assessment and internal use by organizations; (2) clarifying the guidance on using the Framework for supply chain risk management (SCRM) in a more integrated fashion, rather than calling out SCRM as a stand-alone component of the Tiers; (3) expanding and refining the content on authentication and identity management, including

[1] See Draft 2 of Version 1.1 of *the Framework for Improving Critical Infrastructure Cybersecurity* (with markup) https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_with-markup.pdf

[2] See ITI comments in response to NIST RFC - "Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity (Draft Version 1.1)," dated April 10. 2017, at https://www.itic.org/dotAsset/63bc626b-2f2f-4e38-aeaf-31bc6878d2d6.pdf

adding a new subcategory (note we also add a few suggestions for further refinements regarding this topic – see below); and (4) removing the language regarding federal alignment from the Framework in favor of handling this important topic in collateral documentation, as well as the Roadmap. Additionally, we are grateful to NIST for embracing a number of ITI's suggestions regarding the Roadmap, including our recommendations to add items related to the cyber-attack lifecycle, small business awareness and resources, and increased NIST engagement on mapping and aligning the Framework to international standards. Below, we briefly expand on each of these topics, and additionally offer suggestions for further refining and improving Draft 2.

Cybersecurity Measurement

ITI welcomes NIST clarifying the scope and purpose of the new section on measurement as focused on self-assessment. As we mentioned in our comments to the initial draft of Version 1.1, introducing concepts of metrics and measurement can help organizations better define improvements they would like to make to their cybersecurity programs, and communicate these improvements throughout their enterprise and to trusted partners. However, the section on Measurement in the first draft of Version 1.1 suggested NIST was endorsing use of the Framework as a tool for use by *external* third parties, such as auditors, or potentially regulators, to assess or "measure" the efficacy of organizations' cybersecurity programs and practices. We appreciate NIST clarified in Draft 2 that the information generated by organizations for purposes of measurement/metrics is intended exclusively for their *internal* use and reference. Additionally, the focus on self-assessment reinforces that the measurements and metrics contemplated are not intended for external use by policymakers or regulators to evaluate or judge the sufficiency of organizations' cybersecurity risk management programs. Further, we appreciate that NIST embraced our suggestion to kick off a parallel workstream in the Roadmap to continue advancing work on cybersecurity measurement, and we look forward to participating in those discussions with NIST and other stakeholders.

Supply Chain Risk Management

ITI is generally supportive of NIST's changes to Draft 2 integrating simplified guidance on using the Framework for SCRM as a component of the "External Participation" subsection and the "Communicating Cybersecurity Requirements" section, rather than separating out SCRM as a stand-alone component of the Tiers. Addressing global supply chain security concerns has long been a priority for ITI and our members. Indeed, ITI has encouraged the expanded use of the Framework by third-party suppliers in previous public comments, offering several recommendations in this regard, including enacting such requirements through contracts and other *industry-driven* measures. We are pleased to see that Draft 2 retains its focus on industry-driven SCRM standards and best practices. Over the past few years, significant work has been done to mature SCRM standards and best practices, thus the inclusion of SCRM at this stage in the Framework's evolution seems both appropriate and timely. In our comments to the first draft of Version 1.1, we noted the treatment of SCRM primarily as a separate section of the Tiers might be confusing to many organizations, particularly considering the breadth and diversity of organizations using the Framework, and the lack of parity in terms of the places they occupy in the global information technology value chain, and their corresponding roles in SCRM. While we

believe the treatment of SCRM in the "Communicating Cybersecurity Requirements" section does provide clearer guidance to companies regarding how to manage supply chain risks, largely mitigating this concern, we continue to believe the SCRM guidance could be even further simplified integrated throughout the Core, within all relevant Subcategories and Informative References. Finally, we appreciate NIST taking on board our suggestions to further bolster the Informative References with regards to SCRM, including adding international references (*e.g.*, ISO 27000 series) and NIST best practices (*e.g.*, NIST SP 800-161).

Federal Alignment

While ITI welcomed the addition of language in draft Version 1.1 regarding federal alignment to the Framework, and articulating how it can indeed be a helpful tool for use by federal agencies to improve their cybersecurity, we recommended in our comments on the first draft that the development of such guidance within a document outside of but supportive of the Framework itself would be more consistent with and better demonstrate the Framework's broad applicability across sectors and geographies. As such, we were pleased to see NIST remove the Federal Alignment section from the Framework Core in Draft 2. Doing so makes good sense considering several federal requirements now directly apply to how federal agencies implement cybersecurity and the Framework, including the White House's May 2017 Executive Order (EO 13800), which requires each federal agency to use the Framework to manage cybersecurity risk, as well as additional requirements promulgated by OMB and pursuant to FISMA. Further, the Framework is likely to gain more traction internationally with the federal alignment section removed.

Identity Management, Authentication, and Access Control

Overall, we are supportive of the new language to better account for authentication, authorization, and identity proofing in Draft 2, which more accurately reflects the state of the art in identity and access management best practices. in the Framework. However, we suggest that NIST make a couple of additional targeted changes to further enhance the effectiveness of this Category.

Privileged Users. One of the most important areas of IT risk relates to privileged users. Whether inadvertent or malicious, improper actions by privileged users can have disastrous effects on IT operations and the overall security and privacy of organizational assets and information. Therefore, it is essential that administrators be allowed to perform only those actions that are essential for their role—enabling the "least privileged access" for reduced risk. This visibility provides insight on activity and works to prevent or flag anything unusual that indicates security risk. It is important to highlight privileged users, specifically, because privileged user credentials were exploited in the preponderance of recent high-profile hacks, enabling attackers to extract much more sensitive data than non-privileged users would typically be able to access. Specifically, ITI recommends the following change in this regard:

- **Pg. 31: PR.AC-4:** ITI requests that NIST add language regarding "users with enhanced privileges." The new Subcategory language would read: "Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties, *including*

permissions and authorizations for users with enhanced privileges (e.g. IT administrators, CIOs, CISOs, others)."

Analytics. Analytics and risk-based authentication were discussed at the NIST Framework workshop in Gaithersburg in the Spring in both the identity management and access control breakout session, and in the plenary read-out at the end of the workshop. User experience has become more important in the digital economy due to increased demands from consumers and citizens. Security interfaces that are inconvenient and cumbersome often force users into work-arounds, many of which end up violating security policy, sometimes unwittingly.

Risk-based authentication has the benefit of not only facilitating the authentication of the identity but, because of the context that is provided under risk-based models, can also facilitate the recognition of the identity. This means that when there is a better understanding of the context around the identity, such as through geo-location data or purchasing behavior, the system may recognize the identity, determine that traditional authentication is unnecessary based on appropriate risk factors, and allow access. Specifically, ITI recommends the following change in this regard:

- **Pg. 31: PR.AC-7:** NIST added a new subsection focused on authentication, which ITI supports. However, ITI requests that "analytics" be added as one of their examples in the e.g. parenthetical. The new language would read: "Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor, *analytics*) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).

Other Recommendations for Further Refinement of Version 1.1

Cloud Service Providers

Because organizations are increasingly considering cloud service models to accomplish their business objectives, we think it prudent that the Framework more explicitly incorporate the use of cloud computing into the discussion of how organizations communicate with suppliers and make buying decisions. In addition to referencing cloud services as among the architectural options available to organizations as they procure IT products and services, we think organizations undertaking use of the Framework would benefit from considering the potential trade-offs of different technology solutions. Specific suggested changes are provided below.

- **Line 533, Section 2.3, 2nd paragraph.** After the fourth sentence in the paragraph (before the final sentence), we suggest adding the following:

  Profiles can also be used to help organizations have visibility into risks or security benefits resulting from different technology solutions and architecture decisions (e.g., managing their own infrastructure, using different cloud service models, and using managed security services or other vendor solutions).

- **Line 640, Section 3.2, Step 6.** We suggest modifying the third sentence in the paragraph to include a reference to vendor solutions as part of the resources equation, as follows: "The

organization then determines resources, including funding, workforce, *and/or vendor solutions*, necessary to address those gaps.":

- **Line 646, Section 3.2, Step 7:** In the second sentence, after "cybersecurity practices," we suggest adding, *"including by considering potential architectural and vendor changes."* The new second sentence would thus read: "It then adjusts its current cybersecurity practices, *including by considering potential architectural and vendor changes,* in order to achieve the Target Profile."

- **Line 722, Section 3.4, first paragraph:** We suggest adding the following text after the second paragraph (making a new third paragraph):

  For example, Target Profiles can be used to inform decisions about managing technology infrastructure and buying technology solutions, such cloud services, managed security services, or other vendor solutions – e.g., by using the profile to understand how different architectural and technology decisions will affect security boundaries and capabilities and by comparing how different suppliers help organizations meet their security objectives or introduce residual risk that must be addressed.

Threat Modeling and Risk Assessment

Threat modeling can play an important role in helping an organization conduct risk assessments. We recommend adding several Informative References to the Framework Core (Appendix A, Table 2) to better reflect the role of threat modeling in risk assessment, as follows:

- **Pg. 32, ID.RA-1:** We recommend including a reference to NIST SP-800-53 Rev. 4 SA-15 (i.e. Threat Modeling).

- **Pg. 33, ID.RA-3:** Considering that ID.RA-3 provides that "threats are identified," it is reasonable to provide references that would facilitate such identification, such as to threat modeling. We recommend including a reference to NIST SP-800-53 Rev. 4 SA-15 (i.e. Threat Modeling), as well as to NIST SP-800-53 Rev. 4 SA-11 (i.e. Attack Surface Analysis, Static Analysis).

- **Pg. 34, ID.RA-4**: Considering that ID.RA-4 anticipates an organization determining "potential business … likelihoods" of risks, we recommend adding a reference to NIST SP-800-53 Rev. 4 SA-15 as threat modeling provides one means an organization can use to assess such likelihoods.

- **Pg. 34, ID.RA-5**: Organizations can also use threat modeling to help determine risk; we thus also recommend adding a reference to NIST SP-800-53 Rev. 4 SA-15 (i.e. Threat Modeling) here.

Roadmap

The Roadmap, published concurrently with the Framework, serves an important dual role in identifying areas important to improving cybersecurity that are appropriate for future incorporation in the Framework, and those overarching areas deserving of further research and/or industry-led standards

development that are also important to cybersecurity, but will likely continue to be addressed in parallel with the Framework.

We are pleased that several of our recommended additions to the Roadmap are reflected in the most recent draft, including adding a roadmap item focused on the **Cyber-Attack Lifecycle (4.2).** Better understanding the cybersecurity threat intelligence lifecycle is essential for organizations seeking to develop a robust understanding of cybersecurity attacks, which must in turn inform how they calibrate their cybersecurity risk management needs.

We have also consistently advocated that NIST explore mechanisms by which to expand the Framework approach, including urging NIST to explore, with industry stakeholders, the opportunity for submitting relevant parts of the Framework as an international standard. The latest draft of the Roadmap demonstrates progress on this recommendation as part of the **International Aspects, Impacts and Alignment item (4.8),** indicating NIST has actively engaged with the ISO and IEC to map existing international standards to the Framework, work that has led to the anticipated publication of an ISO/IEC Technical Report.

ITI has also previously advocated for a dedicated workstream aimed at helping small and medium sized enterprises (SMEs) better understand and implement the Framework in an efficient and cost-effective manner. We support NIST's inclusion in Roadmap 1.1 of the **Small Business Awareness and Resources** item **(4.12),** which focuses on helping SMEs, many of whom lack mature programs or the technical expertise to keep up with the latest developments in cybersecurity, better understand how to utilize the Framework to more appropriately manage their cyber risks, including through the publication of *NISTIR 7621 Revision 1 - Small Business Information Security.*

Potential Addition to the Roadmap: ***Security by Design/Secure Development***

We encourage NIST to include the concepts of Security by Design, Secure Development Processes or Secure Development Lifecycles (SDLCs) as a roadmap item. Foundationally, we encourage NIST to work with the international standards bodies to recognize existing and further develop security-by-design best practices. Rapid response is critical as the cybersecurity landscape evolves, so to create a trusted digital environment, NIST should seek to encourage companies to tailor security measures and tools to address the risks related to their specific business models and threat profiles, at all SDLC phases.

As a practical matter, several leading technology companies already employ SDLCs and security by design techniques (incorporating security throughout the product development phase) in hardware, devices, and in software. Examples of security that is built into hardware include semiconductor manufacturers designing processor chips with built-in safeguards, or building support for encryption and key management into hardware such as semiconductors, to provide protection against attack. At the device level, for example, companies may enable security options by default or as part of an initial setup process so that users must consciously decide to remove the default protections rather than the opposite—in effect forcing users to improve security on their own.

Regardless of which security measures are taken at the hardware, device, or software level, a holistic view which focuses on the end-to-end security design technique and development lifecycle is far more important than considerations of, for example, the geographic location of where a product is developed.

Secure Software Development Processes and Practices may be the area most ripe for current inclusion in the Roadmap.

Software applications are increasingly integrated into our commercial and infrastructure processes to improve efficiencies. The global economy, critical infrastructure and government operations have increased their dependence on software. However, this makes software applications a prime target for hackers.

As the importance of software has increased, the way software is developed and deployed has continued to evolve. In addition to the importance applications play in our economy, contemporary application development methodologies like DevOps (combining development and operations practices) are increasing the speed and precision with which software is produced and deployed. The ability to create software that can resist modern forms of attack and exploits will be crucial to our ability to protect not just applications, but the social, economic and political processes that depend on that software.

Much software remains insecure in part because many development teams view security as a separate function from software quality. Many organizations fail to integrate security methods into their development lifecycles.

SAFECode (the Software Assurance Forum for Excellence in Code)[3] is a non-profit organization, comprised of leading software development companies, dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. SAFECode develops software assurance guidance publications available for free to the public, outlining software development best practices for developers and organizations. For instance, the SAFECode publication, "Fundamental Practices for Secure Software Development, 2nd Edition,"[4] is designed to help others in the industry initiate or improve their own software security programs and to encourage the industry-wide adoption of fundamental secure development methods.

An emerging ISO Standard, ISO 27034, will provide a basis for independent certification of conformance with software security assurance best practices in the future.

Suggested actions for implementing this proposed Roadmap item include:

- NIST, through the National Cybersecurity Center of Excellence, can partner with leading software assurance organizations, such as SAFECode, and other stakeholders, to develop risk-based, scalable guidance on effective secure software development processes and practices.

[3] https://safecode.org/

[4] https://www.safecode.org/wp-content/uploads/2014/09/SAFECode_Dev_Practices0211.pdf

- NIST can work with international governments to promote policies that enable continued innovation and flexibility in secure software development, while strengthening security.

Conclusion

ITI would like to again thank NIST for its commitment to partnering with the private sector to advance our shared cybersecurity goals. NIST's ongoing commitment to industry outreach is an excellent example of how effective public-private partnership processes can help to improve cybersecurity. More importantly, we would like to again express our appreciation to NIST for not only engaging with stakeholders, but for listening to their feedback and incorporating so much of it into Draft 2.

ITI and its members look forward to continuing to work with NIST, the Administration and international stakeholders to further Framework development and the approach it embodies, as well as on other initiatives to improve our cybersecurity posture. Please continue to consider ITI as a resource on cybersecurity issues, and do not hesitate to contact us with any questions regarding this submission.

Sincerely,

John Miller
Vice President for Global Policy and Law
Cybersecurity and Privacy