From: **John Miller**
Date: Mon, Apr 10, 2017 at 4:53 PM
Subject: ITI comments in response to NIST RFC - “Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity (Draft Version 1.1)”
To: cyberframework <cyberframework@nist.gov>
Cc: "Barrett, Matthew P.", "Sedgewick, Adam"

Attached please find comments of the Information Technology Industry Council (ITI) to NIST’s request for comment (RFC) of January 25, 2017, *Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity*, seeking comments on draft version 1.1 of the Framework for Improving Critical Infrastructure Cybersecurity.

Thank you for the opportunity to provide comments, and please let me know if you have any questions or would like additional information. ITI welcomes the opportunity for further engagement with NIST on the important issue of how best to evolve the Cybersecurity Framework.

Sincerely,

John Miller

John S. Miller
Vice President for Global Policy and Law, Cybersecurity and Privacy
ITI - Information Technology Industry Council
1101 K Street NW, Suite 610
Washington, DC 20005

[Attachment Copied Below]

April 10, 2017

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 RFC - "Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity (Draft Version 1.1)."

Dear Mr. Games:

The Information Technology Industry Council (ITI) appreciates the opportunity to respond to your request for comment (RFC) of January 25, 2017, *Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity*, seeking comments on draft version 1.1 of the Framework for Improving Critical Infrastructure Cybersecurity (hereinafter, "draft Version 1.1").[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. ITI's members comprise leading technology and innovation companies from all corners of the ICT sector, including hardware, software, digital services, semiconductor, network equipment, Internet companies, and companies using technology to fundamentally evolve their businesses. 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 our customers' and 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. policies to be compatible with – and drive – global norms, as well as the potential impacts on our customers. As

---

[1] Draft **Version 1.1** of the Framework for Improving Critical Infrastructure Cybersecurity **(with markup)** https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1-with-markup.pdf

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 long commended NIST's continuing work, in cooperation with the private sector and other stakeholders, to further the development of the voluntary Framework for Improving Critical Infrastructure Cybersecurity (the "Framework" or "Version 1.0"), and draft Version 1.1 represents an important milestone in the Framework's evolution. We are encouraged that NIST took the approach of a "1.1" refinement rather than a "2.0" major revision of the Framework – doing so increases the likelihood of a net expansion of the Framework's meaningful use by a broad array of stakeholders, many of whom may be at different stages of Framework exploration, implementation or use. However, so as not to inadvertently undermine this approach, some of the important items NIST proposes to add to the Framework might be more appropriately developed in workstreams outside of the Framework itself, through the type of robust public-private partnership effort that was a hallmark of Version 1.0's development. ITI continues to support the approach embodied in the Framework, which leverages such public-private partnerships, is grounded in sound risk management principles, and helps foster innovation due to its flexibility and basis in global standards. We commend NIST for its continued leadership in Framework development, and we remain committed to working with NIST to help it succeed.

ITI has not answered each of the questions in the RFC individually, but rather has responded to what we identified as the three natural groupings of questions. In addition, immediately below we offer summary comments and recommendations.

Summary Comments and Recommendations

We offer the following high-level comments and recommendations regarding draft Version 1.1.

Refinement Rather than Wholesale Revision is the Correct Path for Evolving the Framework. As is by now well understood, one of the primary realized benefits of the Framework has been that it provides a common language for a diversity of organizations, their internal stakeholders, and external partners to better understand, communicate and manage cybersecurity risks. ITI previously advocated that global policymakers also stand to benefit from becoming more conversant in the language of the Framework, and cautioned against making drastic changes to the Framework core, as doing so would be the equivalent of scrambling the Framework's alphabet at the same time many are still trying to learn or master the language. On balance, NIST has recognized the need to tread lightly with respect to draft Version 1.1, with an eye toward refinement to make the Framework a more valuable tool to a broader array of organizations, rather than offering a significant expansion that may chill its uptake. While we don't believe the proposed changes in draft Version 1.1 will negatively impact larger organizations that are already using the Framework, for small/medium-sized enterprises (SMEs), the added complexity of, *e.g.*, addressing their organizations' supply chains, may strain resources for those SMEs already using the Framework, and may well serve as a disincentive for those SMEs considering using the Framework.

Highlight the Framework is and Remains a Tool for Flexible, Internal Use by Organizations. Draft Version 1.1 contains helpful language articulating the internal utility of the Framework, as a tool to drive accountability for cybersecurity across organizations, their key personnel, and business partners, to better correlate cybersecurity practices with organizational business objectives and outcomes, and to improve cybersecurity across organizations' supplier ecosystems. However, certain of the revisions in draft Version 1.1, such as the new section on Measurement, might be misconstrued by some to suggest NIST is 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. While it's of course true that some organizations may choose to retain, for instance, external third-party auditors to make such assessments for their own business purposes, doing so may likely be cost-prohibitive for many other organizations. We recommend that NIST clarify that decisions regarding use of the Framework, including for measurement purposes, remain the sole province of organizations.

Clarify the Scope and Purpose of the New Section on Measurement, and Work on Building Consensus in a Parallel Workstream. Introducing concepts of metrics and measurements 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, it is important to stress that much of the data gathered and used by organizations for purposes of metrics or measurement, as contemplated in draft Version 1.1, is likely sensitive, confidential and/or proprietary business data. In addition, this data may be applicable to metrics or measurement in a way that is context dependent and rapidly evolving. We understand that policymakers will appropriately continue to ask, "is the Framework working?" and may well look to the Measurement section in draft Version 1.1 as a "hook" for attempting to "measure" such progress. We suggest NIST identify Measurement as a Roadmap area, and transfer this section to a separate document or set of documents that includes clarifying language to (1) stipulate that the information generated by organizations for purposes of measurement/metrics is intended exclusively for internal use and reference, unless organizations choose to share such information externally, and (2) caution that the measurements and metrics contemplated are not intended for external use by policymakers to evaluate or judge the sufficiency of organizations' cybersecurity risk management programs.

The More Robust Tiers Guidance is a Welcome Addition to the Framework. Draft version 1.1 incorporates additional guidance to explain how organizations can better utilize the Tiers, both in the descriptions of Tiers 1-4 themselves and in the "Seven Steps" for Establishing or Improving a Cybersecurity Program. ITI has previously advocated that NIST beef up the guidance regarding how Tiers should, and should not, be used, so these additions are welcome. The more robust guidance on Tiers incorporated into draft Version 1.1 should help organizations to improve communications regarding cybersecurity progress across their organizations. We recommend adding further clarifications to the Framework to explain that the Tiers are intended to be used internally by organizations –not externally by third parties. Further, we do not believe that supply chain risk management (SCRM), a topical area, is appropriate for inclusion within the Tiers, which should be applicable in assessing levels of investments across relevant risk management functions for all organizations.

Integrating Supply Chain Risk Management into the Framework is Timely, but Must be Done Carefully. Addressing global supply chain security concerns has long been a priority for ITI and our members. While ITI has noted in previous public comments to NIST that some ITI members had begun exploring how to expand Framework use with their suppliers, we cautioned against prematurely incorporating SCRM into the Framework Core at its inception, given the lack of consensus-based industry-led international standards in the SCRM area at the time. 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. However, we recommend simplifying the SCRM language in draft Version 1.1 and integrating it within all relevant Subcategories and Informative References in the Core, rather than including such guidance in the Tiers.

Delineate "Core" from "Adjacent" and "Ecosystem" Roadmap Workstreams. We note that many of the Roadmap areas have not been "addressed" in draft Version 1.1 despite a significant amount of ongoing work and progress, but believe that result is appropriate, given several Roadmap areas lend themselves less toward "incorporation," because they encompass work in overarching areas that will likely continue to be addressed in parallel with the Framework, rather than as part and parcel of it (*e.g.*, workforce challenges). Going forward, we recommend restructuring the Roadmap to reflect different categories of areas for future work – areas for consideration as possible future additions to the Framework Core itself, areas representing important "Adjacencies" relating directly to Framework advancement, and areas impacting the cybersecurity "Ecosystem" more broadly where work must progress in parallel with but "outside of" future revisions of the Framework proper. We encourage NIST to produce such a "Roadmap 1.1" while continuing to evolve draft Version 1.1 – doing so could help rationalize moving some sections that may have been prematurely added to draft Version 1.1 (such as Measurement) to workstreams parallel to the Framework, while still highlighting their importance as adjacencies or to ecosystem cybersecurity, and integral to continued Framework development.

Impacts of Major Framework Updates on Cybersecurity

Question #2: How do the changes made in draft Version 1.1 impact the cybersecurity environment?
In our view, the threshold questions to ask when evaluating any proposed changes to the Framework are the following: will the changes impede the current efforts of diverse organizations at varying stages of Framework exploration, implementation or use, and will the changes help nurture the Framework to expand its meaningful use to a wider array of stakeholders, both in the U.S. and abroad? Informed by this perspective, we previously recommended that NIST and the broader stakeholder community focus on refining and clarifying the Framework, as opposed to vastly expanding it, and we believe draft Version 1.1 is generally consistent with this approach (with the notable exception of the new Measurement section).

The key changes in draft Version 1.1 of the Framework are: (1) a new section on cybersecurity measurement and metrics; (2) expanded guidance on using the Framework for supply chain risk management; and (3) a more robust description regarding the use Implementation Tiers. We address each of these updates in turn below, and provide brief comments on a few smaller refinements.

Measurement and Metrics

The most significant addition to draft Version 1.1 is the proposed new section on cybersecurity measurement in use of the Framework. Introducing the concepts of both metrics and measures (collectively, measurements) can help organizations better define improvements they would like to, and in some cases, may need to make to their cybersecurity programs with greater accuracy, and can help organizations communicate these improvements throughout their enterprise, and their supplier ecosystems. However, it is important for organizations to be able to preserve flexibility in the application of any measurements and metrics. Different organizations face unique threat environments and have different assets, risk tolerances, resources and business priorities. These organizations will appropriately continue to weigh individual Framework subcategories/outcomes differently, and such divergences amongst organizations need to be reflected in how cybersecurity metrics/measurements are used. As such, we recommend that NIST add the nascent area of Measurement/Metrics to the Roadmap for Improving Critical Infrastructure Cybersecurity (the "Roadmap")[2] and continue to develop the concepts in this section in a document or a set of documents external to the Framework, enabling more opportunities for iteration and responding to the needs of communities of interest, including sectors and SMEs.

Turning to the substance of the proposed Measurement section, it expresses what are in our view quite valid objectives, including improving accountability for cybersecurity across organizations, and key personnel within organizations. (p. 21). The section also clearly ties cybersecurity measurement to business outcomes and results, indeed explaining that a major objective is to help organizations better correlate cybersecurity with business objectives. (p. 21). This is a critical clarification of the purposes of explaining the rationale behind cybersecurity measurement, because this is typically not what many policymakers seem to have in mind when they contemplate the use of measures/metrics. NIST should even more explicitly clarify that the purpose of cybersecurity measurement as contemplated in draft Version 1.1 is for organizations' internal use.

One specific clarification that could be made in this regard is to the second sentence of the very first paragraph of the new Measurement section, which reads, "Measuring state and trends over time, internally, through external audit, and through conformity assessment, enables an organization to understand and convey meaningful risk information dependents, partners and customers." (l. 745-747). While this sentence again indicates the purpose of cybersecurity measurement is ultimately to increase an organization's understanding of and ability to communicate cybersecurity risk, the use of the word "and" in line 746 may be misconstrued as implying one purpose of the Measurement section is as a tool to be used by third parties, including external auditors.

We do not believe that NIST conceived the new section on Measurement to endorse use of the Framework measurements and metrics as tools for use by external third parties, such as auditors, or potentially regulators, to assess or "measure" the efficacy of organizations' cybersecurity programs and practices. While it's of course true that some organizations may choose to hire external third-party

---

[2] NIST Roadmap for Improving Critical Infrastructure Cybersecurity, https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf

auditors to make such assessments, doing so may likely be cost-prohibitive for many other organizations, while others may simply prefer to conduct such assessments "in house." We recommend that NIST clarify that decisions regarding use of cybersecurity metrics and measures by organizations should remain within the sole province of organizations. With respect to the cited language, this result could be achieved via minimal edits to the text (*e.g.*, changing "and" to "or" on line 746, and inserting additional clarify language regarding internal decision-making and use).

The proposed Measurement section also acknowledges the complexity involved in correlating cybersecurity metrics to business objectives, citing an example of the interplay between a hypothetical bank's desire to increase online customers (business objective) by implementing stronger authentication (cybersecurity metric). As further illustrated by the example, there are also many other factors in play that may impact the cited business objective and cybersecurity metric, making it difficult to isolate and evaluate the effectiveness of the cybersecurity metric standing alone. This example is helpful in terms of illustrating the challenges of using cybersecurity measures for anything other than internal purposes, given there are so many other factors in play that aren't being "measured" (*e.g.*, messaging, marketing, advertising). Other important complicating factors discussed elsewhere in the Measurement section include cost-effectiveness, as well as the difficulty of "measuring a negative," *i.e.,* that a bad business outcome, such as a data breach, did not happen. (p. 22). Including additional illustrative examples in the Measurement work product could prove helpful in communicating to policymakers and regulators the pitfalls of using cybersecurity measures and metrics for "external" purposes, including as reliable objective indicators of the efficacy of a given organization's cybersecurity program.

The proposed Measurement section concludes by offering several examples of how cybersecurity metrics and measurement could be used to drive increased accountability for cybersecurity across an organization, unquestionably a worthwhile goal. These examples clearly reinforce the internal utility (at the organizational level) of cybersecurity metrics and measurement, because they can be used to hold various personnel across an organization accountable for cybersecurity and/or business outcomes within their zones of responsibility. However, it is important to stress that much of the data used internally by organizations for purposes of metrics or measurement, as contemplated in draft Version 1.1, is likely sensitive, confidential and/or proprietary business data. We suggest NIST include clarifying language in the proposed Measurement section to (1) stipulate that the information generated by organizations for purposes of measurement/metrics is intended exclusively for internal use and reference, unless organizations choose to share such information externally, and (2) caution that the measurements and metrics contemplated are not intended for external use by policymakers to evaluate or judge the sufficiency of organizations' cybersecurity risk management programs.

Supply Chain Risk Management

Addressing security concerns related to SCRM 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. In recognition of the importance of addressing global supply chain security concerns, some companies already have begun exploring how to expand Framework use with their suppliers. One option we have previously offered for consideration is for organizations to include the Framework in their third-party supplier cybersecurity requirements,

provided regulators refrain from directing regulated entities to REQUIRE their suppliers to use the Framework. Two types of instances in which organizations might themselves consider requiring use of the Framework across their supply chains are: (1) where an owner/operator has outsourced the management of any part of its operation via a managed services partnership; and (2) where the supplier is considered a critical business partner, such that any disruption of their business would affect the delivery of critical services. Companies can also take proactive steps to encourage use of the Framework across their ecosystem partners by, for example, integrating the Framework into their supplier guidelines or contracts.

The proposed SCRM language added to Draft Version 1.1 is largely consistent with ITI's previous recommendations. Draft Version 1.1 adds language articulating the importance of communicating and verifying cybersecurity requirements across organizations' supply chains, as well as guidance seeking to help organizations determine cyber requirements for suppliers and partners, and suggests enacting such requirements through contracts and other industry-driven measures. (pp. 17-18). We agree an industry-driven approach is the right approach to addressing SCRM, given the interrelated importance of cross-border data flows and global value chains to the global business community. Unfortunately, policies that have the effect of restricting global commerce are currently *en vogue* around the globe, including forced localization or "country of origin" requirements, both of which often masquerade as having some abstract security benefit, but neither of which offer a tangible security benefit from a risk management standpoint. To guard against similar motivations inspiring global policymakers to potentially proffer prescriptive and similarly deleterious SCRM requirements, we support the inclusion of industry-driven SCRM standards and best practices in draft Version 1.1.

However, including such SCRM guidance in the Tiers seems misplaced and may be confusing to many organizations because such guidance is not broadly applicable across the diversity of organizations using the Framework, undermining the Framework's relevance across sectors and organizations. SCRM, as a topical area, is inappropriate for inclusion within the Tiers, which should be applicable in assessing levels of investments across relevant risk management functions for all organizations. Instead, we recommend simplifying the Framework's SCRM guidance and integrating it throughout the Core, within all relevant Subcategories and Informative References.

While the Informative References have been significantly bolstered with regards to SCRM, with several standards added to draft Version 1.1 (pp. 30-31), there are other international references (*e.g.*, ISO 27036) and NIST best practices (*e.g.*, NIST SP 800-161) that could also be added. ITI previously cautioned against prematurely incorporating SCRM into the Framework at its inception, given the lack of consensus-based industry-led international standards in the SCRM area at the time. Over the past few years, given that significant work has been done to mature SCRM standard and best practices, the inclusion of SCRM at this stage in the Framework's evolution – provided it is done in the right way – seems both appropriate and timely.

Tiers

ITI commented previously that while establishing current and target profiles was a useful activity, there was scant guidance in Version 1.0 regarding how to examine, use, or reconcile multiple current or target profiles, and that the text of the implementation tiers sometimes created overlapping metrics,

potentially leading to subjective risk determinations. While flexibility is certainly key, particularly as organizational risk objectives vary greatly, promoting certainty and confidence in decision making are also important. We advised NIST to consider developing greater clarity around what distinguishes one tier from another to provide a more useful frame of reference for Framework users, and specifically recommended expanding the definitions of the Tiers to include additional detail and usage notes. We were pleased to see draft Version 1.1 incorporates ITI's previous suggestions in this regard.

Draft version 1.1 helpfully incorporates additional guidance to explain how organizations can better utilize the Tiers, both in the descriptions of Tiers 1-4 themselves and in the "Seven Steps" for Establishing or Improving a Cybersecurity Program (pp. 15-16). The more robust guidance on Tiers incorporated into draft Version 1.1, including to tie cybersecurity risk to business objectives (p. 11); their use and sharing of cybersecurity threat indicators (p. 9); and language explaining the robustness of communications between stakeholders within an organization calibrated to different Tiers (pp. 11-12) will no doubt prove helpful to organizations using or considering using the Framework.

Consistent with our comments above regarding Measurement and SCRM, however, we do believe further clarifying guidance is warranted to make clear the Tiers are primarily intended to be used by organizations for internal purposes. ITI previously commented that, without a common methodology for how tiers are determined and without a statement on the scope of how they may be used, in particular by external parties, the tiers could create unintended anticompetitive consequences. Because draft Version 1.1 still lacks a methodology for how to calculate and apply Tiers, they should not provide a basis to compare one organization to another. However, Tiers nonetheless are likely to become factors in procurement and purchase contracts. Further, some ITI members have voiced concerns that the Tiers may be used by CI owners and operators to try to push liability onto their vendors. For example, despite the voluntary nature of the Framework, a CI owner or operator nonetheless could require in its contracts that its vendors be "Tier 4," even if that is otherwise an unnecessary level for those vendors, and use that stipulation to shift blame onto vendors in the event something goes wrong. Such potential usage of the Tiers runs counter to the idea that the Tiers represent a maturity model, that different Tiers will be appropriate for different businesses, and that the tiers should be self-determined based on a company's posture vis-à-vis CI and its own organizational goals.

To preserve the intended flexibility of Framework use and to minimize such unintended consequences, ITI suggests NIST prioritize developing language explicitly explaining why the type of external use of Tiers described above would be inappropriate, and specifying that the tiers are for internal use only as part of an organization's cybersecurity risk management process. Additionally, NIST should consider developing a methodology for determining Tiers, perhaps as part of the continuing work on metrics and measurement, as supplemental guidance. ITI companies stand ready to contribute ideas and expertise to NIST to try to create such a workable methodology for determining and using tiers.

Other changes/additions of note

Federal Alignment**.** ITI has previously provided comments to NIST promoting the Framework as a common language for policymakers that can help align US federal agency cybersecurity and risk management efforts by orienting them toward the Framework, and help expand use of the Framework globally. The explicit 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, is a welcome addition (p. 20). However, 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.

Authentication and Identity. The refinements to better account for authentication, authorization, and identity proofing more accurately reflect the state of the art in identity and access management best practices, which will have a positive impact on the cybersecurity ecosystem. (p. 32). ITI has previously recommended prioritization of and further development of Authentication and Identity standards and technologies, and their incorporation into the Framework core as related standards and best practices reach a sufficient level of maturity and consensus. As standards and best practices in this area continue to evolve and mature, we would be supportive of including them in the Framework.

Cyber Threat Information Sharing. We note with appreciation that cyber threat indicators and information sharing have been incorporated into draft Version 1.1, including in the enhanced guidance regarding Tiers (p. 9), risk assessment (p. 15), and the Incorporated References (p. 29). Adding this area to the Roadmap was a previous recommendation submitted to NIST by ITI.

Privacy. Draft Version 1.1 contains new language stating that "cybersecurity activities create risks to privacy." (p. 19). No further explanation is offered with respect to this change. While it is true that certain cybersecurity activities might create risks to privacy, if organizations implement proper risk management controls such risks can be mitigated if not eliminated. Indeed, from ITI's perspective, an organizational risk management program should optimize for both cybersecurity and privacy. We recommend adding clarifying language around this addition, to avoid the perception that cybersecurity activities always create risks to privacy.

Questions regarding Scope of Proposed Update, Impacts on Framework Use

1) Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?
3) For those using Version 1.0, would the proposed changes impact your current use of the Framework? If so, how?
4) For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the Framework? If so, how?
6) Is there a better label than "Version 1.1" for this update?

To reiterate, ITI believes any proposed changes to the Framework should be viewed from the following perspective: will the changes impede the current efforts of diverse organizations at varying stages of Framework exploration, implementation or use, and will the changes help nurture the Framework to expand its meaningful use to a wider array of stakeholders, both in the U.S. and abroad? Informed by this perspective, NIST seems to have by and large struck the right balance in terms of incorporating additional guidance, best practices, and standards in areas where a sufficient level of consensus and maturity has been reached. While additional topics of will continue to emerge in an area as dynamic as cybersecurity, we believe NIST has been judicious in not adding more than the Framework stakeholder

community can reasonably be expected to digest in an update at this time (with the notable exception of the proposed new section on Measurement). We do not recommend adding further topics to Version 1.1; rather, we suggest NIST focus on adding important clarifying language, as suggested above, to more accurately and completely characterize the updates that have already "made the cut," And to earmark certain additions as proposed updates to the Roadmap requiring parallel workstreams.

While we don't believe the proposed changes in draft Version 1.1 will negatively impact larger organizations that are already using the Framework, for small/medium-sized enterprises (SMEs), the added complexity of addressing their organizations' supply chains may strain resources for those SMEs already using the Framework, and may well serve as a disincentive for those SMEs considering using the Framework. One important caveat to the above statement involves the area of Measurement. While it's possible some may view the Measurement section as seemingly opening the door to and possibly calling for costly third-party audits, we believe if clarifications along the lines we suggested above (*i.e.*, that measurement/metrics are intended for internal use) are made, this concern can be mitigated. Moving this section out of the Framework proper will do much to help in this regard.

With respect to the name for the Framework update, we believe "Version 1.1" hits the mark as it is more appropriately reflective of refinement, rather than the type of major revisions "Version 2.0" might imply. A broader point for NIST and the stakeholder community to consider, however, involves the full name of the Framework itself – the Framework for Improving Critical Infrastructure Cybersecurity. Given the increased uptake of the Framework beyond the CI community, including by federal, state and local government entities, and considering the addition of SCRM in draft Version 1.1, it seems clear to us that the Framework is being used and is impacting organizations of all types and sizes as a risk management tool. Considering this reality, we question whether "Critical Infrastructure" should continue to be included in the document's title.

Questions Regarding the Roadmap

5) Does this proposed update adequately reflect advances made in the Roadmap areas?
7) Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap?
8) Are there any areas that should be removed from the Roadmap?

All the areas identified in the Roadmap, published concurrently with the Framework, were and remain important to improving cybersecurity, and further research and /or industry-led standards development work in these areas will prove very helpful. However, and consistent with our prior public comments, we have consistently cautioned against adding any new functions, outcomes, or informative references to the Framework Core until they have sufficiently matured and gained broad industry acceptance and adoption. The barometer for adding topics to the Framework Core should thus be whether there are sufficiently developed consensus-based, industry-led international standards and best practices in these areas (other than adding language that seeks to clarify how the Framework can be efficiently and effectively used).

In general terms, NIST seems to have struck the right balance in terms of focusing additional guidance, best practices, and standards in areas where a sufficient level of consensus and maturity has been

reached. Roadmap areas such as **SCRM** and **Authentication** more readily lend themselves to integration into the Framework Core (as indicated by the additions to draft version 1.1) We note that many other of the Roadmap areas have not been explicitly "addressed" in draft Version 1.1 despite a significant amount of ongoing work and progress, but believe that result is on balance appropriate, given several Roadmap areas don't easily lend themselves to "incorporation," in large part because they represent overarching areas that will likely continue to be addressed in parallel with the Framework, rather than as part and parcel of it (*e.g.*, **Cybersecurity Workforce**).

One notable exception to this generalization are Roadmap areas calling for "Alignment" (specifically, relating to Federal Agency or International alignment). While these areas are on their face not intended to be integrated into the Framework proper, ITI did previously recommend prioritizing these two "alignment" Roadmap areas for inclusion in Framework updates. While draft Version 1.1 does include a brief section addressing "**Federal Agency Cybersecurity Alignment**," we note there was no such reference to "**International Aspects, Impacts, and Alignment**," despite the significant expenditure of effort and progress on this front by not only NIST, but also industry partners.

ITI has previously highlighted many of the reasons why international alignment efforts around the Framework are essential. Promoting the Framework will help the U.S. to sustain its leadership on cybersecurity around the world, and this will in turn help to further enhance the Framework's use within the United States. To facilitate further global adoption, NIST and its Federal agency partners should continue to promote the Framework approach with their global government partners, and NIST should make some reference to these efforts in draft Version 1.1.

Other Roadmap areas, such as "**Cybersecurity Workforce**," clearly have much broader cybersecurity ecosystem impacts beyond the Framework, and despite both meaningful progress and acknowledgement of ongoing challenges, probably don't warrant and may not ever warrant being included in the Framework proper.

Going forward, we believe NIST would be well-advised to restructure the way in which the Roadmap areas are presented, to better delineate which areas are **"Core"** Roadmap areas that may be included in the Framework Core, which represent important **"Adjacent"** Areas relating directly to future Framework advancement (such as areas calling for alignment), and which areas are more accurately identified **as "Ecosystem"** Roadmap areas that are important to advancing cybersecurity progress more generally.

Potential Additions to the Roadmap

As NIST looks forward to how best to evolve and mature the Framework, it should certainly consider adding other areas to the Roadmap.

There are other key elements necessary for informed risk management that should also be on NIST's radar – for instance, the **cybersecurity threat intelligence lifecycle**, which is essential to developing a robust understanding of cybersecurity attacks. While NIST has initially added some references to cyber threat incident sharing in draft Version 1.1, much more work could potentially be done to better integrate this area into the Framework.

NIST should also consider other mechanisms by which to expand the Framework approach. For example, given the increasing global acceptance of the Framework, we would support NIST exploring, with industry stakeholders, the opportunity for submitting relevant parts of the **Framework as an international standard**. This could be a valuable contribution to further harmonizing cybersecurity practices on a global scale. Today more than 80 countries are in the process of creating new cybersecurity regulations and there are myriad implementing requirements being considered. Adding the Framework as an international standard could help propagate a standards-based and more aligned approach globally, supporting both U.S. economic advancement and security. NIST could also invest more substantially in promoting the Framework and the public-private partnership approach through which it was developed internationally with governments and its peer standards organizations.

A dedicated workstream aimed at **helping SMEs understand and implement the Framework** in an efficient and cost-effective manner also seems worthwhile. Not all companies have mature programs or the technical expertise to keep up with the latest developments in cybersecurity – such as the Framework – to appropriately manage cyber risk. SMEs, for example, have reported being confused and even overwhelmed by the size and complexity of Framework 1.1, and some will doubtless be even more confused when they learn there will soon be a Framework 1.1. Given the interconnected nature of the cyber ecosystem, ITI is keenly aware that cyber elements of the critical infrastructure can be compromised by weaknesses in smaller entities to which they are technologically connected. Given this fact, it is critical for us to create a sustainably secure cyber ecosystem for all entities, large and small. We recommend that NIST work with interagency partners including the Department of Homeland Security (DHS), the Small Business Administration, and Sector Specific Agencies to better understand the cybersecurity and implementation challenges faced by organizations of all sizes, and consider ways to make the Framework more approachable for all organizations. NIST should prioritize understanding the issues confronting theses smaller entities and addressing their unique concerns and needs as part of "Roadmap 1.1."

A final area where there is a currently a substantial amount of activity involves **Internet of Things (IoT) Security**. While it is clearly premature to consider adding any of the outputs from the many ongoing IoT security workstreams to the Framework, identifying IoT Security as A Roadmap area will help ensure NIST is prepared to add any consensus best practices, guidelines and standards to the Framework at such time or soon after they sufficiently mature and gain consensus amongst stakeholders.

CONCLUSION

ITI would like to again thank NIST for its commitment to partnering with the private sector to advance our shared cybersecurity goals. We would also like to extend to the new Administration a willingness and eagerness to continue to work together with NIST and other federal government partners to improve cybersecurity together. NIST's ongoing commitment to industry outreach is an excellent example of how effective public-private partnership processes can help to improve cybersecurity.
As NIST and other stakeholders evaluate draft Version 1.1 over the coming months, we continue to believe that the changes contained therein should be evaluated through consideration of whether the changes increase the value of the Framework as a risk management tool to current users, and expand

the Framework's meaningful use to a broader diversity of stakeholders. The proposed updates included in draft Version 1.1 generally seem to strike the right balance in terms of refinement rather than vast expansion, and the upcoming Framework workshop in May will provide the first of what we hope are a series of excellent opportunities to discuss whether the changes proposed in draft Version 1.1 accomplish these overarching goals. We encourage continued Framework engagement by NIST and other stakeholders, particularly internationally, where we have observed a strong and growing interest by governments in multiple countries.

ITI and its members look forward to continuing to work with NIST and the Administration to further Framework development and the approach it embodies, and on other initiatives to improve our cybersecurity posture. Please continue to consider ITI a resource on cybersecurity issues moving forward, 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