February 23, 2016

Diane Honeycutt
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 RFI - "Views on the Framework for Improving Critical Infrastructure Cybersecurity"

Dear Ms. Honeycutt:

The Information Technology Industry Council (ITI) appreciates the opportunity to respond to your RFI of December 11, 2015, "Views on the Framework for Improving Critical Infrastructure Cybersecurity."

ITI is the global voice of the tech sector. We are the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry, and this year we are pleased to be commemorating our centennial. 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 is critical to our members' success—the protection of our customers, our brands, and our intellectual property is an essential component of our business, and impacts our ability to grow and innovate in the future. 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. As a result, we 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 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 commends 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"). The Framework 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 believe the Framework has already helped and will continue to help improve cybersecurity, and we remain committed to helping it succeed.

ITI has endeavored to answer the questions in this RFI from the perspective of ITI itself as a multiplier organization (a trade association) and/or as an aggregated response from our member companies, as indicated below. We have not answered each of the twenty-five questions individually, but rather have responded to each of the four question sets. In addition, immediately below we offer some summary comments and general observations.

Overarching Observations: Refining the Framework, Expanding its Use, Fostering Guidance

We commend NIST for its continued leadership in Framework development, including by seeking to understand how the Framework is being used, and how best to evolve it and share lessons learned based on an informed understanding of what is working and what can be improved. While it is important to stress that we are still in the early phase of a multi-year effort, it is not too early for NIST to continue to push the conversation and the Framework forward by exploring these important areas, to continue to build momentum behind the Framework. We offer the following high-level observations regarding how best to focus our collective efforts on the topics probed in the RFI.

Focusing on Framework use – by organizations and policymakers – is timely and warranted. The questions regarding use in the RFI are important, as we understand that patience is short amongst policymakers of all stripes who expectedly want to know – "is the Framework working?" But discussing the benefits of Framework use, and attempting to judge the usefulness of the Framework by, for instance, quantifying the number of Framework users, are two very different things. As NIST is well aware, cybersecurity is not an end state—we can never be 100% secure in cyberspace due to ever-evolving threats, technologies, and business models. Cybersecurity is a process of dynamically managing risks amidst these constant changes, and while the Framework embodies this approach, it is not the only tool in the cybersecurity risk management toolbox. So while counting the number of entities using the Framework may be tempting, doing so will not ultimately demonstrate whether those

stakeholders are managing cyber risks more effectively. Rather, providing qualitative evidence of the Framework's beneficial uses to organizations is more instructive, and we have aggregated such indicia of use below.

Promoting the use of the Framework as a policymaking tool deserves greater focus. As we detail below, while the Framework has frequently been lauded as providing a common language which can help companies and other organizations better communicate risk management to improve cybersecurity internally (for instance with company executives or boards) and externally across their ecosystems (such as with business partners including suppliers), the potential of the Framework to provide a common language or taxonomy for policymakers globally, and at all levels of government, has not yet been fully realized. In particular, promoting the Framework as a common language for policymakers 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.

Framework updates should focus on refinement rather than expansion. Given that the Framework needs to gain traction with a broader diversity of stakeholders to more fully realize its potential as a risk management tool, and we are advocating that global policymakers stand to benefit from becoming more conversant in the language of the Framework, it seems premature to make drastic changes to the Framework core itself. So as NIST and other stakeholders consider updates, we need to tread carefully, with an eye toward refinement to make the Framework a more valuable tool to a broader array of organizations, rather than significant expansion that may chill its uptake.

Sharing best practices can help produce usable guidance. While there are a number of private sector organizations who have embraced the Framework and are utilizing it for the benefit of their own enterprise risk management practices and security systems, some of the value of these positive experiences is lost if their results are not shared with industry and government partners. Because all stakeholders can benefit from our shared experiences and understanding, NIST and other stakeholders should increase efforts to build communities of practice. In particular, focusing on turning the experiences of the "early Framework utilizers" into usable guidance stands to provide the most benefit to organizations who haven't had the expertise or resources to "test drive" the Framework, such as small and medium size businesses (SMBs).

NIST can convene a dedicated process to explore long-term governance options. Looking ahead to future governance is an issue NIST has consistently addressed since before the Framework was even published. Yet at the same time, it is difficult to separate the Framework's early success from the NIST-convened process that created it, and NIST's stewardship since. As the primary users and consumers of the Framework, the private sector ultimately owns the Framework. But we shouldn't underestimate the continuing importance of

NIST's role as convener, and custodian, of not only the Framework, but also the governance conversation. The smartest way to explore the future governance of the Framework is for NIST to convene focused discussions amongst stakeholders in the same thoughtful manner as that which produced the Framework itself.

Question Set 1: Use of the Framework

ITI's members are major multinational companies that have understood and managed cybersecurity risks for decades. Our companies build risk management into their ongoing daily operations through legal and contractual agreements, cybersecurity operational controls, cybersecurity policies, procedures, and plans, adherence to global risk management standards (including many of those listed as informative references in the Framework), and a host of other practices. Many operate 24x7 network operations centers (NOCs) and participate in a host of entities that help them to understand and manage their risks, such as Sector Coordinating Councils (SCCs) and information sharing and analysis centers (ISACs). We are confident that many large, multinational companies are similar to ITI companies in these ways.

Our own baselines of understanding notwithstanding, we believe the Framework is having an important, valuable impact on organizations' understanding of cyber risks. As we describe below, the Framework has in some cases allowed ITI companies to have useful conversations about cybersecurity risk management both internally (e.g. with our senior management) and externally (e.g. with boards of directors, partners, suppliers, and customers), allowing these parties to better understand the importance of managing cyber risks. The Framework's common terminology (identify, prevent, detect, respond, recover) provides a common, standardized language to enable these discussions.

Nearly all of ITI's member companies were involved with the development of the Framework in some fashion, and many are using, or planning to use, the Framework (or its constituent components), in various ways as described below.

Examples of Framework Use – Realized Benefits to Companies

One company reported utilizing the Framework to assess, prioritize, and improve their cybersecurity program. This company initiated its use of the Framework by conducting an internal mapping of their cybersecurity program controls, helping the company to become familiar with the terminology and approach of the Framework. The company's leadership team felt it was important to conduct an independent assessment, as doing so would help provide an objective picture of their overall cybersecurity posture. To test the Framework, this company contracted with a major third party consulting firm to assess their controls against the categories and subcategories of the Framework. Their information security team is currently reviewing the recommendations and action plans produced from the review with

company leadership, and intends to implement continuing improvements to its cybersecurity plan in the coming year.

Another ITI company reported that, while no specific element of the Framework itself led to improved or enhanced capabilities, their review of the Framework itself was beneficial, as it led to broader conversations across the company. By bringing experts together to review alignment to the Framework, they identified opportunities for consistency of approaches and improved sharing of information. In addition, the discussions yielded an unexpected detection solution innovation, based on convening company experts to discuss existing capabilities and brainstorming on new capabilities.

Another ITI member reported multiple benefits as follows:

- *Improved harmonization of risk methodology and language:* The Framework has been effective in enabling a common risk management methodology and language across internal stakeholder communities.
- *Low cost to use:* Because the Framework is based on existing industry practices, the Tiers, Core elements, and common vocabulary were easy to learn and to use by the company's internal stakeholders and facilitated uniform, accurate, and rapid assessments across disparate domains of risk. Further, to date the company has found the development and use of related tools and training to be low-cost.
- *Improved visibility into risk landscape:* One unexpected benefit came from mapping the assessments of the same Core items by various subject matter experts (SMEs) in a single risk "heat map" – this enabled quick identification of outliers, significant differences, and visibility issues regarding the organization's risk landscape. They intend to similarly map results from various business units and anticipate visualizing certain organizational trends and groupings. "These new insights would not have come nearly as easily without a unifying mechanism like the Framework."
- *Risk tolerance discussions among decision makers:* One of the most valuable benefits came from the internal discussions regarding actual and target tiers, including discussions and comparisons of strategies across domains as they relate to the company's enterprise risk goals. The discussions helped foster common agreement between stakeholders and leadership on risk appetite and strategic issues, which in turn is helping to guide the organization in security project prioritization and funding.

Other ITI companies reported finding the Framework's mapping to ISO/IEC 27001 and NIST SP 800-53 as Informative References to be helpful, as these standards established an immediate linkage between the companies' ongoing risk management and certification efforts. This type of mapping provides an extremely helpful example to share with governments outside of the United States that may be considering their own national cybersecurity frameworks/initiatives.

By mapping the Framework's security guidance to global standards, NIST has demonstrated that national cybersecurity concerns can be addressed in a manner that bolsters global standards.

Another ITI company reported it is piloting a program to align its enterprise cybersecurity management to the Framework and is introducing Framework concepts and integrating applicable portions into certain internal risk management and governance processes. The company noted it has made these alignments without negative impacts to existing project planning or roadmaps, and expects that over time the balance of its security programs and projects will have substantially aligned their risk management processes to the Framework. The company also reported it has found adopting the Framework's approach in areas with already strong cyber risk management practices and culture incurs very low program management overhead. The company estimates it has invested less than 150 total work-hours (across a multinational company with 100,000+ employees) at about the halfway point of its enterprise-wide pilot. Along the way they have developed a small set of tools, lightweight processes, and training aids for better process repeatability, so "additional efforts may take even less overhead."

Companies have begun exploring how to expand Framework use with their suppliers. One ITI company noted two instances in which it believes owners and operators of critical infrastructure (CI) services should want to require the Framework of their supply chains: (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. Another company has begun taking steps to encourage use of the Framework across its ecosystem partners by integrating the Framework into its supplier guidelines.

Promoting Use of the Framework by Policymakers

The Framework has consistently been lauded for providing a common language for companies, to better help them comprehend, communicate and manage cybersecurity risks. The Framework's common language is grounded in consensus best practices and international standards, better equipping organizations to better discuss risk management and cybersecurity internally (for instance with company executives or boards) and externally across their ecosystems (such as with business partners such as suppliers). However, it's clear that the common language of the Framework can also be promoted and better used to provide a common language or taxonomy for policymakers globally and domestically, at all levels of government. Amongst other benefits, doing so can help prevent duplication of regulatory efforts.

As NIST pointed out in the Framework document itself, "Executive Order [13636] called for the development of a voluntary, risk-based Framework – a set of industry standards and best practices to manage cybersecurity risks." That is exactly what NIST produced, with significant input from industry, in the Framework, and we do not suggest that NIST or other stakeholders lose sight of the inherent "voluntariness" of the Framework, or stop promoting it as such. However, this is not to say that we should ignore the reality that government policymakers and, yes, regulators –internationally, at the U.S. federal level across various agencies, and at the state and local level – are increasingly looking to the Framework for inspiration as they consider whether and how to exercise their regulatory authorities to help improve cybersecurity. Indeed, this inevitability was anticipated in Sec. 10 of the Executive Order, which clearly contemplated the opportunities the Framework created for "regulatory streamlining," and White House cybersecurity coordinator Michael Daniel subsequently indicated the Administration was "beginning a process to identify federal regulations that were excessively burdensome, conflicting or ineffective."[1]

While a report on the Administration's regulatory streamlining efforts to date is expected sometime this month, we believe more can and should be done to reinforce the Framework as voluntary, while at the same time embracing its sensible use by regulators to streamline and on a net basis reduce cybersecurity regulations. How can we accomplish this? The key is that the Framework should not serve as the impetus or rationale for extra layers of regulation – that's not regulatory streamlining, it's regulatory redundancy, and it won't create better cybersecurity for anyone, including regulated entities themselves. Rather, the Framework can still be held up as a voluntary risk-management based tool, while also serving as a beacon around which policymakers at every level – including regulators – should orient their efforts to improve cybersecurity. Doing so in turn will help reduce regulatory redundancy.

As a starting point for domestic alignment efforts, NIST should work with its interagency partners to drive alignment of cybersecurity requirements for Federal information systems with the cybersecurity outcomes of the Framework. A majority of information security vendors service both the public and private sectors. Aligning Federal Information Security Management Act requirements with the Framework subcategories, and mapping these requirements to other global standards referenced in the Framework, will enable more vendors to compete in the public and private sector information security marketplaces, driving further innovation and improving security capabilities.

[1] Michael Daniel, "Strengthening Cyber Risk Management," Feb. 2, 2015. Retrieved from https://www.whitehouse.gov/blog/2015/02/02/strengthening-cyber-risk-management

Question Set 2: Possible Framework Updates

As we consider whether and how to most effectively update the Framework, ITI believes any proposed changes should be viewed from the following perspective: 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 recommend NIST and the broader stakeholder community focus on refining and clarifying the Framework, not expanding it, as follows.

Clarifying the Framework Core

While many entities around the country (and likely the world) may be familiar with the importance of identifying assets in their IT systems and protecting them (the first two steps in the Framework Core), some ITI companies observe that more needs to be done to drive home the importance of the last three steps in the Core—detect, respond, and recover—and what entities can do in these areas. As NIST and others in the administration have said many times, the Framework is not meant to stop all cybersecurity incidents, some of which will continue to occur. However, the Framework can help entities prepare, detect, respond, and recover earlier when incidents happen. We suggest that these latter three phases warrant NIST's focus as it evolves the Framework, and offer some concrete suggestions below.

Profiles. The Framework's core is a helpful structure for developing risk management processes, stimulating useful processes across organizations, and establishing relatable internal benchmarks. But the simplicity of the Framework sometimes limits its use across more complex organizations. For example, establishing current and target profiles is a useful activity; however, there is little available guidance regarding how to examine, use, or reconcile multiple current or target profiles. We recommend NIST add considerations to the supporting materials to better enable tailoring the steps in Section 3 to organizational capabilities, and for tailoring the Categories and Subcategories to the organizational environment.

Tiers. Similarly, the text of the implementation tiers sometimes creates overlapping metrics, which may lead 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. Developing greater clarity around what distinguishes one tier from another could provide a more useful frame of reference for many Framework users.

Specifically, we recommend expanding the definitions of the Tiers, including additional detail and usage notes. There are at least two reasons for this.

First, not all parts of the Framework lend themselves to a tiered approach, as some are yes/no type objectives.

Second, while we applaud the concept of a maturity model in the Framework, 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 the Framework does not outline a methodology for how to calculate and apply them, tiers do not provide a basis to compare two organizations. However, tiers nonetheless are likely to become factors in procurement and purchase contracts. Further, some ITI members have voiced concerns that the Framework implementation tiers will 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 if something goes wrong. Such potential usage of the tiers runs counter to the very 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 the company's posture vis-à-vis CI and its own organizational goals.

To try to minimize such unintended consequences, ITI suggests NIST include in the next version of the Framework language explicitly explaining why this type of external use of Tiers would be inappropriate, and specifying that the tiers are for internal use only as part of an organization's cybersecurity risk management process. NIST also should include in Version 2.0 a methodology for determining tiers. ITI companies stand ready to contribute ideas and expertise to NIST to try to create a workable methodology for determining tiers.

Informative References. In addition, risk management standards, as well as the threat environment itself, are constantly evolving. Accordingly, it seems appropriate that the list of informative references should be reviewed and updated on a periodic basis. However, consistent with the high bar that was set for inclusion in Framework 1.0, only informative references that comprise consensus-based, industry-led international standards and best practices should be considered for inclusion in future Framework updates.

Addressing the Roadmap

All of the areas identified in the Roadmap for Improving Critical Infrastructure Cybersecurity, published concurrently with the Framework, are important to improving cybersecurity, and further research and /or industry-led standards development work in many of these areas could prove very helpful. However, consistent with our above recommendations, we caution against adding any new functions, outcomes, or informative references to the Framework Core until they have matured and gained broad industry acceptance and adoption.

Put another way, a recommendation against including a given Roadmap topic in the next iteration of the Framework should not be construed a judgment that important work doesn't need to be advanced on that or other Roadmap areas. For example, the importance of continuing our collective research and standards development efforts in areas such as authentication and supply chain risk management cannot be overstated. However, we believe it is premature to incorporate topics such as these in the Framework, due to the lack of developed consensus-based, industry-led international standards and best practices in these areas. We encourage NIST to continue working with stakeholders to help promote development of standards in these areas, something we note NIST is already doing in other contexts, such as in the recently published "Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity," which helpfully articulated the need to develop new standards in several important core areas of cybersecurity standardization.

In terms of prioritizing Roadmap areas for inclusion as Framework updates, two identified areas that strike us as ripe for inclusion in the next iteration of the Framework, are "Federal Agency Cybersecurity Alignment" and "International Aspects, Impacts, and Alignment."

Federal Agency Cybersecurity Alignment. As noted above, it is extremely important to push for alignment of federal agency cybersecurity practices, including orientation of federal agency efforts to the Framework, which will in turn facilitate mapping of agencies' cybersecurity risks to their missions government-wide. In fact, we understand the White House has directed federal agencies to use the Framework, and that many are doing so. The Administration should consider developing guidance for federal agencies applying the NIST Framework to help them use business drivers to guide cybersecurity activities and consider cybersecurity risks as part of their risk management processes. In other words, the federal government or another agency should develop government-wide recommendations as government "sector-specific guidance" in the manner in which many other sectors (such as the financial and energy sectors) currently are developing for themselves. Perhaps more importantly, as also noted above, any regulatory efforts by those same agencies should be streamlined to reduce regulatory redundancy – providing Administration guidance aimed at orienting any such efforts toward the Framework is the surest way to accomplish this.

International Impacts and Alignment. We have already discussed above many of the reasons why international alignment is essential. A foundational aspect of driving such alignment involves the global Framework promotion efforts of both industry and government. As a sector, we have supported organizations across the globe who are using the Framework as the basis to assess their actual cybersecurity risks. The Framework is gaining traction internationally, and familiarity is growing in multiple geographies. Specifically, international use

of the Framework is gaining support in the following sectors: Financial, Electric Utilities, Water Utilities and Oil and Gas. Furthermore, the Framework is being used to establish security requirements and as a way to recommend threat mitigation controls and remediation. Promoting the Framework in its current form will help the US 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 promote the Framework approach with their global government partners. For example, the Department of State should reference the Framework in all of its global cybersecurity capacity-building efforts. Likewise, the White House should highlight the Framework in its strategic cybersecurity partnerships. International acceptance of industry-led, global cybersecurity standards will help drive even greater competition and innovation in the global marketplace.

Beyond the Roadmap. As NIST looks forward to how best to evolve and mature the Framework, it shouldn't limit itself to the areas identified in 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.

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 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 approach globally.

Question Set 3: Sharing Information on using the Framework

ITI is comprised of many of the largest ICT companies in the world. While a number of our companies, and those in other sectors, have embraced the Framework and are utilizing it for the benefit of their own enterprise risk management practices and security systems, some of the value of these positive experiences is lost if the results are not shared with industry and government partners. Because all stakeholders can benefit from our shared experiences and understanding, NIST and other stakeholders should increase efforts to build communities of practice, to facilitate the sharing of this knowledge. In particular, focusing on turning the experiences of the "early Framework utilizers" into usable guidance stands to provide the most

benefit to organizations who haven't had the expertise or resources to test drive the Framework, such as SMBs.

Developing implementation guidance for SMBs

We recognize 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. SMBs in particular have reported being confused and even overwhelmed by the size and complexity of the current Framework. Given the interconnected nature of the cyber ecosystem, we are 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. Therefore, in the next phase of Framework development, 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.

At the end of the day, the goal of such guidance efforts, simply stated, is to help make it easier for a broader diversity of organizations to use the Framework. These practices could help organizations better assess how the array of actions embedded in the Framework can best be leveraged to meet the requirements and risk tolerances of organizations of various sizes across numerous industry segments. With this knowledge in hand, and by also factoring in business needs including cost effectiveness, organizations may be more likely to adopt processes that they know they can afford and are more readily applicable to their particular risk environments.

Additionally, ITI and our member companies continue to work with a range of organizations to receive information and share lessons learned about the Framework. In the U.S., ITI has worked extensively to share Framework best practices from a "policy perspective," both though our involvement with the Communications Security, Reliability and Interoperability Council (CSRIC), and also through our collaboration with a cross-sectoral group of associations dedicated to advancing and developing the Framework approach.

Prioritizing global Framework outreach

Outreach to international audiences, including the sharing of best practices, should also be significantly enhanced. It is particularly important that foreign governments who are carefully watching the Framework's development better understand its approach. Many governments around the globe are at pivotal points in their own cybersecurity policymaking—examples

include the EU's Network and Information Security (NIS) Directive, which will soon be formally ratified and then must be implemented by all 28 EU member states, and cybersecurity policies and laws at different stages of development across Asia and Latin America. However, many foreign governments and foreign audiences generally still do not understand the Framework's voluntary, risk management approach or its rationale, and mistakenly believe NIST is writing new standards for the U.S. economy. Thus, international outreach that focuses on the facts underlying the Framework and the approach it embodies will continue to be essential. Conducting such outreach in local languages (e.g. with the assistance of our Embassies abroad) would be extremely helpful.

For our part, ITI has conducted significant Framework outreach to international audiences. For example, ITI staff and some of our member companies visited Beijing, Seoul, and Tokyo and shared with these countries' governments and business leaders the benefits of a public-private partnership-based approach to developing globally workable cybersecurity policies. ITI highlighted the Framework as an example of an effective policy developed in this manner, reflecting global standards and industry-driven practices.

Additionally, since the release of the Framework, ITI has participated in discussions with government officials visiting Washington from Israel, India, and China, focusing on many of these same points. For example, ITI arranged for a presentation on, and discussion of, the Framework with China's cybersecurity standards development body, TC260. We have subsequently conducted additional Framework outreach in China, as well as in Germany and India.

Question Set 4: Private Sector Involvement in Governance of the Framework

Since the publication of the NIST Roadmap for Improving Critical Infrastructure Cybersecurity in February 2014, NIST has consistently raised the question of whether governance of the NIST Framework should be transitioned to a private sector organization. For now, we recommend that NIST, as a non-regulatory federal entity with expertise in convening diverse stakeholders, continue to play a leadership role in the promotion and maintenance of the Framework. However, given NIST's demonstrated interest in this topic, perhaps NIST can engage with the private sector to drive more focused discussions to weigh the options for long-term Framework governance.

One idea worth exploring is the creation of a cross-sector industry advisory panel, tasked with developing and implementing a governance plan. To ensure the long-term success of the Framework, we believe an ongoing, formal strategic dialogue between NIST and the various industry sectors could best position a future governance model that helps the Framework evolve in a way that is beneficial to all stakeholders.

One model such a panel could consider is what an industry-driven non-profit organization taking over the long-term governance of the Framework would look like. There is precedent for this; a similar model already exists for the Smart Grid and NSTIC IDESG efforts. This model has the dual advantages of an independent, non-governmental body steering the process and the private sector taking the lead on steering it.

Another approach such a panel might consider is one focused on identifying which attributes are most desirable for any subsequent governance organization. Attributes that might be explored include:

- an international mandate and global recognition and respect as a subject matter expert;
- the ability to support various implementation approaches/activities across the global cyber ecosystem;
- expertise across multiple sectors;
- demonstrated objectivity;
- commitment to engaging with a broad stakeholder community, including the private sector; and
- dedicated, professional staff with technical risk management capabilities.

An organization possessing the above attributes might be well-positioned to work with governments around the world to further develop the Framework and refine it for international standardization. In any event, given NIST has already indicated it would rather not be responsible for the Framework development process long term, and that we share NIST's international aspirations for the Framework, the governance model needs to be addressed in a focused manner sooner rather than later.

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 commend the Administration for its willingness and eagerness to consistently engage with our companies and the ICT industry generally to determine how government and industry can best work together to improve cybersecurity. The commitment to industry outreach is an excellent example of how effective public-private partnership processes can help to improve cybersecurity.

As we look forward to what comes next for the Framework, any changes should be made with an eye toward nurturing it to expand its meaningful use to a broader diversity of stakeholders. This can be accomplished in three primary ways: (1) by refining the Framework to improve its utility to a wider array of stakeholders; (2) by sharing best practices to provide more usable guidance; and (3) by promoting the Framework's use as an orientation point amongst global policymakers, to better align divergent or overlapping policy/regulatory efforts. 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, Global Cybersecurity and Privacy Policy