Information Technology Industry Council

October 14, 2014

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: "Experience with 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 August 26, 2014, "Experience with the Framework for Improving Critical Infrastructure Cybersecurity."

ITI is the premier voice, advocate, and thought leader in the United States for the information and communications technology (ICT) industry. ITI's members comprise the world's leading innovation companies, with headquarters worldwide. Cybersecurity is rightly a priority for all governments. We share the goal with governments of improving cybersecurity and therefore our interests are fundamentally aligned. As both producers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy. Further, our members are global companies located in various countries. Most service the global market and have complex supply chains in which products are developed, made, and assembled in multiple countries across the world. 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.

ITI commends NIST's work leading the development, in cooperation with the private sector and other stakeholders, of the voluntary Cybersecurity Framework. The Cybersecurity Framework leverages public-private partnerships, is based on sound risk management principles, and will help preserve innovation because it is flexible and based on global standards. We believe the Framework can help improve cybersecurity, and we are committed to helping it succeed.

ITI has endeavored to answer each question 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, depending on the nature of the question. At the same time, we have not answered every question and we have copied below in bold those to which we are responding. In addition, immediately below we offer some general comments and observations.

Overarching Observation: We are at an Early Stage

We commend NIST for seeking to understand what is working and what can be improved. At the same time, it is important to stress the Cybersecurity Framework was released only eight months ago and we are just at the beginning of a multi-year effort.

Overall, our companies are seeing the right set of things at this point to illustrate that the marketplace is accepting the Cybersecurity Framework and the effort is meeting the intent of the Executive Order (EO), despite a challenging cyber threat environment. It is important to put into context that we are seeing myriad benefits from a spectrum of activities associated with the development of the Framework. The workshops and related events brought together multiple sectors to work on a common task, which has fostered and/or augmented cross-sectoral discussions and collaborations on cybersecurity risk management—essential activities given our growing interdependencies. The activities associated with the Framework also have helped to foster a growing culture of cybersecurity risk management, and the market is responding with new products and services around the Framework to help entities of all sizes manage those risks.

As such our focus and expectations should be appropriate, realistic, and will by necessity change over time, and we must focus on gauging the right things, in the right order, particularly as this effort unfolds. Promoting the Framework is not the sole goal – rather, it is promoting better cybersecurity risk management and resilience. While information captured via this RFI will be extremely helpful to sharing initial lessons and prioritizing next steps—and understanding where improvement is needed—answers must be reviewed and analyzed in the context of the early stages of a tremendous endeavor.

Thus, the RFI's questions rightly begin with awareness. Since releasing the Framework in February 2014, NIST and the administration generally have correctly focused on raising awareness of the Framework and how it can be used to manage cyber risks. As ITI stated in February 2014, a meaningful demonstration of efficacy in the first year is the amount and nature of the government's outreach and awareness campaign, and stakeholder participation from the defined target audience(s).[1] If stakeholders are unaware of the Framework, use will be limited. Further, while the Framework references existing standards and best practices, it presents them in a new way, which may require some time for organizations to internalize. Therefore, NIST and its partners in the federal government should continue to focus on outreach and awareness efforts in the short term.

The questions on experience (use) are important, but also must be put into context. Again, the goal is not "adoption" of the Framework. 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. Further, the Framework is but one tool in cybersecurity risk management. Counting the number

[1] *ITI Recommendations to the Department of Homeland Security Regarding its Work Developing a Voluntary Program Under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity,"* February 11, 2014, found at http://www.itic.org/dotAsset/3ed86a62-b229-4d43-a12b-766012da4b1f.pdf.

of entities using the Framework may be tempting, but will not ultimately demonstrate whether all stakeholders are managing cyber risks more effectively.

We hope our answers are helpful in capturing information at this point in time and we expect the answers will change as awareness and use of these tools continues to grow. To that end, we recommend that NIST ask these types of questions again in a year so that we can see how experiences evolve.

Question Set 1: Current Awareness of the Cybersecurity Framework

1. What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations? Six months after the Framework was issued, has it gained the traction needed to be a factor in how organizations manage cyber risks in the Nation's critical infrastructure?

ITI's 59 member companies are major multinational companies, nearly all of which have been involved with the development of the Framework in some fashion and are aware of it. Thus, ITI will answer this question from the perspective of how our member companies are seeing awareness manifested among other entities with which they work.

Awareness among customers: Some ITI companies report they are receiving inquiries from their customers on the Framework. These inquiries include 1) requests for help understanding what the Framework is; 2) how to use it; 3) if the ITI company (as a vendor) has products or services that map to the Framework; and 4) how the ITI company's products or services can help the customer use the Framework. These inquiries come from customers of all sizes, including private entities (in both regulated [e.g., banking] and non-regulated sectors), government customers at the federal, state, and local levels, and international customers—although one ITI company reports their global technology group has not been getting inquiries from customers about the Framework from outside of North America.

2. How have organizations learned about the Framework? Outreach from NIST or another government agency, an association, participation in a NIST workshop, news media? Other source?

We are answering this question first from the perspective of ITI itself as a multiplier organization (a trade association) and then as an aggregated response from our member companies.

As an association, ITI has learned about the Framework directly from NIST and via participation in a NIST workshop.

Most ITI companies have learned about the Framework directly from NIST or another government agency (e.g., via direct communications or speeches), and from participating in NIST workshops. In some cases ITI companies have gained additional details through sources

such as ITI and other trade associations, news publications, standards development organizations, congressional inquiries, and sector-specific Framework implementation guidance initiatives. Some ITI companies report their customers, suppliers, partners, and others are learning about the Framework through various sources, including ITI companies' own outreach. See more details in our response to Part I's Question 8.

3. Are critical infrastructure owners and operators working with sector-specific groups, non-profits, and other organizations that support critical infrastructure to receive information and share lessons learned about the Framework?

Yes. ITI and our member companies are working with a range of organizations to receive information and share lessons learned about the Framework. Some examples are below.

- Communications Security, Reliability and Interoperability Council (CSRIC): ITI and a number of ITI companies are members of the CSRIC.
- Informal consultations with other associations: ITI is sharing information on a regular basis with a range of associations in various industries, including in finance, energy, telecom, health care, manufacturing, and others. In fact, ITI spearheaded original efforts to gather together a cross-sectoral group of associations and individual companies, starting from April/May 2014, to discuss our efforts regarding the Framework and cybersecurity risk management. This informal group has grown to involve additional sectors and continues to informally share information and experiences developing or disseminating information on the Framework, as well as experiences working with NIST, our sector-specific agencies (SSAs), and/or other departments or agencies to promote use of the Framework and cybersecurity risk management generally.

4. Is there general awareness that the Framework:
a. Is intended for voluntary use?
b. Is intended as a cyber risk management tool for all levels of an organization in assessing risk and how cybersecurity factors into risk assessments?
c. Builds on existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity?

We will first provide an overall response and then respond separately to parts a, b, and c.

There is some awareness about all of the parameters above, but much more must be done to raise awareness about them, both inside and outside the United States. Both ITI as an association and many of our member companies individually are making concerted efforts to continually explain these key facts. For example, some ITI member companies report they emphasize these facts when hosting webinars or doing other outreach. As an association, ITI makes these points regularly to international audiences in the course of our global outreach, as do many of our members given their large global footprints and reach. ITI and our companies plan to continue to regularly and strongly convey these facts and urge NIST and the administration to do so as well so that awareness of them will grow.

These facts need particular increased emphasis vis-à-vis two key audiences: the press, and international audiences. We will elaborate on these points below, and we continue our discussion of the importance of international audiences in our response to Part I's Questions 6 and 9.

4a. Is there general awareness that the Framework is intended for voluntary use?

The Framework's voluntary nature is still not widely understood and is in some cases confusing. Further, voluntary for whom, and by whom, are key points. The Framework is being used not only by the private sector (where use truly is voluntary) but also by federal, state, and local governments. For some government entities, use is not voluntary. In fact, the White House and Department of Homeland Security (DHS) have made clear that U.S. federal government agencies must use the Framework, and some state and local governments are requiring their agencies and departments to use it. These usages, which ITI supports, do not detract from the Framework being voluntary for industry, but we need to sharpen our descriptions and distinctions to avoid confusion or skepticism. In addition, some sectors are developing Framework implementation guidance—we need to emphasize that such activities are voluntarily undertaken by industry actors that find the Framework useful and that such guidance is not a form of federal government mandate.

In addition, some ITI companies report hearing uncertainty about whether regulatory agencies will reference components of the Framework Core in their regulations, which could have the effect of making the Framework compulsory. We encourage NIST and the administration to continue expressing that the Framework is intended to be utilized within existing regulatory authorities, and does not bring with it any new regulatory authority.

The messaging on the voluntary nature of the Framework also is getting muddied by some reporters, bloggers, scholars, industry representatives, and others who question the Administration's intentions or state that the Framework simply by its existence is a step toward regulation. We must counter those suspicions and accusations.

4b. Is there general awareness that the Framework is intended as a cyber risk management tool for all levels of an organization in assessing risk and how cybersecurity factors into risk assessments?

This is still not widely understood, which may be tied to a general lack of understanding that the most effective approach to cybersecurity is based on risk management, and that the Framework reflects this approach. The Framework is not meant to stop all incidents, which will continue to happen even with robust risk management programs. The Framework can help entities protect themselves but also help them detect incidents and respond and recover earlier to them if—or more likely when--they happen.

We continue to hear that some people mistakenly believe the informative references (the standards and best practices enumerated in the Core) are a laundry list of requirements. We must

continue to emphasize the informative references are merely examples across the spectrum of cybersecurity risk, are not necessarily appropriate to the needs of every organization, may not capture all standards and practices used by all entities, and are not required.

4c. Is there general awareness that the Framework builds on existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity?

Some ITI members report growing awareness of this fact in conversations with their customers as well as international policymakers. Some ITI companies are also seeing a greater emphasis in sector-specific publications stressing how the Framework is meant to build off of and complement existing cybersecurity practices, rather than replace them. However, confusion remains and this point needs continual reinforcement by NIST, DHS, and other agencies.

Below we describe some specific confusions we observe.

Confusion that NIST wrote new standards: Many audiences continue to think NIST (or the U.S. government generally) wrote new standards and guidelines for the Framework. This confusion may stem in part from the public's greater familiarity with NIST's more traditional role in cybersecurity (where NIST does develop cybersecurity standards and guidelines with industry for U.S. federal information systems, as required by the Federal Information Security Management Act (FISMA)) and less familiarity with NIST's other, distinct role as a convener of stakeholders to work voluntarily on certain issues, such as with the National Strategy for Trusted Identities in Cyberspace (NSTIC), the smart grid, and now the Framework. Confusion is likely magnified by the press, although many news outlets and reporters have refined and corrected their messaging over time. Regardless of reason, NIST and the administration generally must refine, sharpen, and repeat messaging on this point.

Confusion with other risk management "frameworks:" Some ITI member companies report hearing confusion about how the Framework relates to other existing "frameworks" or cybersecurity-related guidance.

5. What are the greatest challenges and opportunities—for NIST, the Federal government more broadly, and the private sector—to improve awareness of the Framework?

One challenge identified is that of helping organizations and their leaders understand the importance of cybersecurity risk management in an organization's business practices—including the potential costs to an organization if it is hit by a successful cyber incident. NIST and the administration can continue to work with industry to help educate critical infrastructure (CI) owners and operators on the role of cybersecurity in business risk management overall.

Another company noted challenges related to how the Framework is meant to relate to, or be used by, entities not considered CI. The Executive Order and Framework were motivated by a desire to address cyber risks to CI, although the Framework notes it can be applicable

everywhere, including non-CI entities. This results in some ambiguity for non-CI entities in terms of how they should approach the Framework and if they should use/follow it. The company reports they currently see a tendency by those non-CI entities (those "not clearly falling under the Framework") to have low understanding of the Framework and dismiss it as not applicable to them. The company observes that these sectors were generally not involved in the drafting of the Framework (since it seemingly started as an exercise applicable only to CI sectors) and do not have the level of familiarity with it that CI sectors do. Some education and outreach to non-CI sectors may be in order.

At the same time, the company reports concern among some of these non-CI sectors about publically talking about using the Framework for fear it may open the door to some sort of CI designation (or *de facto* self-designation) and subject them regulatory regimes that apply (or may apply in the future) to CI.

6. Given that many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, what is the level of awareness internationally of the Framework?

ITI as an association performs extensive global work on cybersecurity policy and has had many discussions with international colleagues about the Framework. In addition, ITI's members are major multinational companies and thus many of them have insight into this question.

We believe international awareness is at a decent level. Some ITI companies report references to the Framework outside of the United States, whereas other companies do not, although some think it is well known among the international expert community.

Two challenges internationally are as follows:

- Understanding about the Framework's focus on voluntary risk management—and why we chose that approach-- remains low. We believe this results largely from a difference in regulatory culture: many foreign countries have traditions of greater command-and-control by the government of the economy in general and of standards development in particular. As a result, a frequent assumption is that a government would of course internally develop country-specific and mandatory cybersecurity standards, rather than work, as NIST did, in a true partnership with industry to develop voluntary guidance on the basis of international standards and best practices. This cultural difference is why it is important to repeatedly and clearly communicate to foreign audiences about the nature of the Cybersecurity Framework.
- Some ITI companies report that the Snowden disclosures and the related tarnishing of U.S. technology policies is creating a stumbling block to the international community assessing the positive aspects of this U.S. initiative.

Below are some of our specific observations on international awareness.

Asia

- China
  - Some key Chinese stakeholders with whom ITI works are aware of the Framework, although understanding of its voluntary approach is low.
  - There is interest by China's cybersecurity standards development body, TC260, to adopt parts of the Framework for a similar type of guidance in China.
- Korea
  - Based on some meetings we had in Seoul in May 2014, we felt awareness is at a nascent stage among the Korean government, namely the Korea Internet and Security Agency (KISA). During the same trip we felt awareness was raised among Korean firms.
- Japan
  - Based on some meetings we had in Tokyo in May 2014, we felt awareness seemed high within some key parts of the Japanese government (National Information Security Center [NISC], Ministry of Economy, Trade, and Industry [METI], and Ministry of Internal Affairs and Communications [MIC]. In fact, a unit of METI translated the Framework into Japanese in May 2014, as NIST is aware.[2] During the same trip we felt awareness was decent among major Japanese multinationals of the Framework and its approach.

International awareness and understanding of the Framework (its goals and its voluntary nature) is critical. Many foreign governments are carefully watching the Framework and might emulate our approach in their policy environments.

7. If your sector is regulated, do you think your regulator is aware of the Framework, and do you think it has taken any visible actions reflecting such awareness?

Our sector is not regulated and therefore does not have a regulator.

8. Is your organization doing any form of outreach or education on cybersecurity risk management (including the Framework)? If so, what kind of outreach and how many entities are you reaching? If not, does your organization plan to do any form of outreach or awareness on the Framework?

We are answering this question first from the perspective of ITI itself as a multiplier organization (a trade association) and then as an aggregated response from our member companies.

ITI's outreach

Because ITI's membership does not include any small companies and because ITI is a policy-focused association, ITI generally does not do education and training for our members. Nonetheless, we think it is important that stakeholders understand the Framework and why we support the public-private partnership-based approach to developing globally workable policies.

[2] http://www.ipa.go.jp/files/000038957.pdf

Our outreach to date is as follows.

Domestic outreach

- On October 1, ITI held a "Cybersecurity Summit" in Washington DC, one panel of which included representatives from a range of industry sectors discussing their efforts to promote the Framework and management of cyber risks generally.

International outreach

Given ITI's strong focus on global cybersecurity policy, as an association ITI has focused our outreach to international audiences.

- In May 2014, 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.
- ITI is currently contemplating visits to other capitals this coming fall and winter.
- Since the release of the Framework, ITI has participated in discussions with government officials visiting Washington from Israel, India, and China, focusing on the same points described in the first bullet above. For example, ITI arranged for a presentation on, and discussion of, the Framework with China's cybersecurity standards development body, TC260, in September 2014.

<u>ITI member companies' outreach</u>

Some ITI companies report conducting awareness and outreach in the following manners:

- As active participants in standards development organizations that have published Framework implementation guidance.
- By holding webinars on the Framework and its contents and/or and on the products and services the companies offer to help their customers use the Framework.
- By holding events on the Framework and its policy implications.
- By speaking at public conferences, seminars, and other events in the United States and internationally.
- By arranging for NIST to speak at events, such as on a panel at the QuEST Forum's Americas Best Practices Conference in September 2014.
- By directly engaging in policy outreach with foreign government policymakers—such as in Japan and the EU--as those governments consider their approaches to cybersecurity in CI.
- By speaking about the Framework to the media.

Some ITI companies report they plan to continue to provide outreach on the Framework.

9. What more can and should be done to raise awareness?

NIST can help by supporting industry-led efforts to raise awareness and education levels on the Framework and by working with its federal agency partners to coordinate sector-specific outreach and education workshops on it. NIST can also encourage SSAs and other departments/agencies to use their websites to improve visibility and promotion of the Framework and to include more sector-specific content regarding it.

Further, we should increase our efforts vis-à-vis two key audiences: small- and medium-sized businesses (SMBs) and international audiences.

SMBs: SMBs comprise the vast majority of entities in the United States. SMBs are key drivers of growth, employment, trade, entrepreneurship, and innovation in the U.S. economy and thus improving their cyber resilience will benefit our economy generally. In addition, regardless of whether particular SMBs are CI, they are key links in the cyber ecosystem overall as suppliers, vendors and customers, and also simply by nature of being online. Thus, SMBs' cybersecurity and resilience can indirectly impact CI owners and operators and other entities in our economy.

We know of a smattering of activities focused on this audience, such as the U.S. Chamber of Commerce's roadshow to various cities around the country, as well as some outreach the U.S. government is doing to the SMB audience. However, such outreach must increase significantly. ITI previously recommended that DHS, via its Critical Infrastructure Cyber Community (C^3) voluntary Program, conduct outreach and raise awareness vis-à-vis SMBs along three key dimensions:[3] 1) helping SMBs understand cybersecurity threats so they can make informed decisions based on their unique risk profiles; 2) communicating to all entities, including SMBs, that the Framework and the Program exist (and are voluntary), and the existence and availability of both DHS and private sector capabilities of which companies can avail themselves to learn how to use the Framework to assist with their cybersecurity risk management; and 3) helping SMBs understand the range of existing federal agencies and programs available to help small entities manage their cyber risks and invest in the appropriate products and services, people, and processes to address these risks. These agencies/programs include, but certainly are not limited to, the Small Business Administration (SBA)'s *Cybersecurity for Small Businesses* program, NIST's Hollings Manufacturing Extension Partnership (MEP), NIST's National Cybersecurity Center of Excellence (NCCoE), and DHS's own *Stop.Think.Connect.* Campaign.

International audiences: Outreach to international audiences must also be significantly enhanced. It is particularly important that foreign governments who are carefully watching the Framework's development understand its approach. Many governments are at pivotal points regarding their own cybersecurity policymaking—examples include the EU's draft Network and Information Security (NIS) Directive, Germany's draft Cybersecurity Law, and cybersecurity policies being contemplated by the new Modi government in India. However, many foreign

[3]These recommendations were in ITI's March 26, 2014 response to DHS's "Request for Information: Cyber Security Solutions for Small/Medium Sized Businesses, Solicitation # RFI20140220," found at http://www.itic.org/dotAsset/22a9bbda-df11-403f-9b52-531212b9c521.pdf

governments and foreign audiences generally still do not understand the voluntary, risk management approach (and why) and mistakenly believe NIST is writing new standards for the U.S. economy. Thus, international outreach that focuses on our approach and facts about the Framework is essential. To the extent this can be done in local languages (e.g. with the assistance of our Embassies abroad) it would be extremely helpful.

Question Set 2: Experiences with the Cybersecurity Framework

1. Has the Framework helped organizations understand the importance of managing cyber risk?

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 in our response to Part II's Question 8 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 for these discussions.

2. Which sectors and organizations are actively planning to, or already are, using the Framework, and how?

ITI represents 59 major multinational ICT companies. This portion of the ICT sector is planning to use, or using, the Framework, in various ways as we describe below.

3. What benefits have been realized by early experiences with the Framework?

Some ITI companies report that even in initial efforts they have seen benefits, including several unexpected ones, to utilizing the Framework.

One 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 some 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 company reported the unexpected benefit resulting 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 their 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: The company reported that 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 enterprise risk goals. This fostered common agreement between stakeholders and leadership on risk appetite and strategic issues, which can guide the organization in security project prioritization and funding.
    - The company reported that "For this reason, we strongly advise against using Tier Targets established by outside agencies or third parties, as pre-made targets would pre-empt relevant and necessary internal dialogue with an organization regarding risk and prioritization."

4. What expectations have not been met by the Framework and why? Specifically, what about the Framework is most helpful and why? What is least helpful and why?

Helpful:

- One ITI company reported finding the Framework's mapping to ISO/IEC 27001 and NIST SP 800-53 to be helpful, as it established an immediate linkage between the company's ongoing risk management and certification efforts.
- The mapping also continues to provide 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.

Needs work:

- 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, and as we reiterated in our response to Part I's Question 4b, the Framework is not meant to stop all incidents. Incidents will continue to happen. The Framework can help entities prepare, detect, respond, and recover earlier if incidents happen. We suggest that these phases be key areas of focus in NIST's outreach as well as work in the roadmap and/or Framework Version 2.0.
- The Framework does not contain a scope, so how it could be applied is wide open, which could have unintended consequences in supply chain relationships. One ITI company noted two instances it believes owners and operators of 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.

5. Do organizations in some sectors require some type of sector specific guidance prior to use?

The IT sector has not issued sector-specific guidance, and we cannot comment on the needs of other sectors.

6. Have organizations that are using the Framework integrated it with their broader enterprise risk management program?

One ITI company reported it is piloting a program to align its enterprise cybersecurity management to the Framework and is introducing the 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."

7. Is the Framework's approach of major components—Core, Profile, and Implementation Tiers—reasonable and helpful?

Core: This component is reasonable and helpful.

Profile: This component is reasonable and helpful.

Implementation Tiers: This component of the Framework is still confusing for a few reasons.

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 are 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 would be inappropriate, and specify 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.

8. Section 3.0 of the Framework ("How to Use the Framework") presents a variety of ways in which organizations can use the Framework.

We will first provide an overall response and then respond separately to parts a through f.

As NIST and others in the administration have stated, many entities have very robust cybersecurity processes and programs that may already accomplish much if not all of what is outlined in the Framework. ITI's members are major multinational companies with decades of experience in cybersecurity and fall into these categories. At the same time, many ITI companies are finding the Framework useful in a variety of ways, as described below.

a. Of these recommended practices, how are organizations initially using the Framework?

Some ITI companies report their processes were already quite similar to NIST's recommended practices in Section 3.0 of the Framework. One company reported that, following the release of the Preliminary Framework, and again after the release of the final Framework, it leveraged the Framework as part of its own enterprise risk management program. Its largest cloud services also conducted service-level assessments against the Framework to examine their alignment. Because the ITI company already has a robust focus on cybersecurity and privacy in its enterprise and service-level risk management programs, and because the Framework's informative references draw from long-standing security standards, the Framework's security guidance was fairly easy to digest by the company's security risk management professionals. The company also then briefed the results of its assessment to many different groups and components across the company, including sales, legal, and government affairs, providing them with the basic tools necessary to answer questions and talk to customers.

b. Are organizations using the Framework in other ways that should be highlighted in supporting material or in future versions of the Framework?

We recommend NIST add these items to the supporting materials:

- Considerations for tailoring the steps in Section 3 to the organizational capabilities.
- Considerations for tailoring the Categories and Subcategories to the organizational environment.
- Expanding the definitions of the Tiers, with additional detail and usage notes. However, NIST must work closely with all stakeholders on this- see our answer to Part I Question 7, above.

c. Are organizations leveraging Section 3.5 of the Framework ("Methodology to Protect Privacy and Civil Liberties") and, if so, what are their initial experiences? If organizations are not leveraging this methodology, why not?

NIST incorporated the privacy methodology in Section 3.5 as part of the Framework Core (instead of in an Appendix) to make it clear that organizations using the Framework should consider the potential impacts of their cybersecurity activities on individual privacy and civil liberties throughout their cybersecurity risk management practices. ITI companies are committed to ensuring their customer information is afforded appropriate privacy protections and ITI supports the Framework's current methodology as supporting these efforts.
An ITI company stated they have long integrated their security and privacy risk-management

functions, and thus the Section 3.5 approach has been useful as it aligns with both the company's existing security and privacy risk management practices.

d. Are organizations changing their cybersecurity governance as a result of the Framework?

As noted above in our response to Part II, Question 1, ITI's members are major multinational companies that have understood and managed cybersecurity risks for decades.

e. Are organizations using the Framework to communicate information about their cybersecurity risk management programs—including the effectiveness of those programs—to stakeholders, including boards, investors, auditors, and insurers?

Some ITI companies are using the Framework to communicate risk information to immediate stakeholders such as boards of directors, practitioners, and managers. Some note they plan to use the Framework to communicate to more stakeholders eventually, although work will be needed to determine the methods and characterizations needed to do that, especially straightforward visualization of the complex results.

f. Are organizations using the Framework to specifically express cybersecurity requirements to their partners, suppliers, and other third parties?

Some ITI companies plan to, as they see the ability to express requirements via a common language is one of the Framework's key benefits.

9. Which activities by NIST, the Department of Commerce overall (including the Patent and Trademark Office (PTO); National Telecommunications and Information Administration (NTIA); and the Internet Policy Taskforce (IPTF)) or other departments and agencies could be expanded or initiated to promote implementation of the Framework?

We will focus our answer not just on activities related to the Framework, but expand our recommendations to other activities that NIST/Department of Commerce (DOC) overall or other departments and agencies should take to promote better cybersecurity risk management and resilience in the United States. Overall, as described below, we think NIST/DOC should certainly undertake activities aimed at industry outside of CI.

Framework:

- Outreach to SMBs. As we described in Part I's Question 9, a number of NIST/DOC units—MEP, NCCOE—as well as SBA already work closely with SMBs on cybersecurity, and they should intensify their work to inform SMBs about the Framework and other cybersecurity risk management tools. DHS can assist with these efforts, as we explain.
- Interagency awareness. The White House should expand its discussions with all departments and agencies to continue to inform and educate them that the Framework is

currently part of the government's official policy on cybersecurity and is something they should be promoting and/or aligning with. We hear from some ITI member companies that government-wide understanding of this fact is still lacking in some quarters.

- Industry-led guidance. NIST, the SSAs, and other department/agencies should promote industry-led Framework implementation guidance initiatives, including showcasing them on easily accessible federal web sites.
- Regulated sectors. SSAs that currently regulate their sectors for cybersecurity should update (but not add to) current sector-specific regulations with the Framework's lexicon.
- International outreach/travel. NIST and the administration should continue and augment international travel to discuss the Framework with foreign governments and industry.
- Framework 2.0. Because we are at an early stage with Framework 1.0—in terms of raising awareness and determining how it is being used—we recommend that NIST not yet turn its attention to developing version 2.0.

Non-Framework:

- Revisit 2011 Cybersecurity Green Paper. There are many other essential roles NIST/DOC should play in cybersecurity policy outside of the Framework in coming years. Particularly given DOC's primary role in the administration to promote economic growth and innovation—both of which underpin cybersecurity—the Department should be a key contributor to, and in many cases driver of, federal cybersecurity policies. For example, NIST/DOC should revisit some of the ideas put forward in the Internet Policy Task Force's "Cybersecurity, Innovation, and the Internet Economy" draft paper (AKA "Green Paper") released in 2011. ITI responded to a number of the questions during the public comment period on that Green Paper and we have copied those recommendations and ITI's responses in an attachment to this letter.[4]

10. Have organizations developed practices to assist in use of the Framework?

As producers of ICT products and services, some ITI companies have taken many steps to assist others in using the Framework.

- Some ITI companies are developing new products and services to help others use the Framework and manage cyber risks and improve their resilience.
- Some ITI companies have mapped their current products and services to the Framework's specific functions (identify, protect, detect, respond, recover) and controls. One company reported two resulting benefit of this tooling: 1) it allows them to maintain a consistent, repeatable, cross-company approach to assessing how they line up against the Framework and 2) this cross-company approach has generated enhanced collaboration and coordination across internal groups, focusing attention on integrating solutions for customers.

[4] "ITI comments: Response to Department of Commerce Cybersecurity, Innovation, and the Internet Economy Green Paper Notice of Inquiry," submitted August 18, 2011, found at http://www.itic.org/dotAsset/b84c1859-cfa6-4c1a-9145-6c5cccfd1c72.pdf

- Related to product and services noted above, some ITI companies have developed basic sales and informational and marketing materials detailing how their offerings can help customers achieve cyber risk management objectives vis-à-vis the Framework.
- Some ITI companies are developing new products and services specifically aimed at SMBs' use of the Framework/managing cyber risks.
- Finally, some ITI companies have developed internal tools, light-weight processes, and training materials to aid their internal alignment to the Framework.

Question Set 3: Roadmap for the Future of the Cybersecurity Framework

1. ***Does the Roadmap identify the most important cybersecurity areas to be addressed in the future?***

The nine areas identified in the Framework's Roadmap for future work are:

4.1 Authentication
4.2. Automated Indicator Sharing
4.3. Conformity Assessment
4.4 Cybersecurity Workforce
4.5. Data Analytics
4.6. Federal Agency Cybersecurity Alignment
4.7. International Aspects, Impacts, and Alignment
4.8. Supply Chain Risk Management
4.9. Technical Privacy Standards

With respect to NIST's interest in whether its Roadmap is focused on the right areas for further development, ITI companies generally feel the Roadmap's substantive focal points are correct. All of these areas are important to improving cybersecurity, and further research and /or industry-led standards development work in many of them could be very helpful. However, we caution against adding any new functions, outcomes, or informative references to the Framework Core until they have matured and gained broad voluntary industry acceptance and adoption.

We have comments on some of the areas, as follows.

- ITI strongly supports prioritizing the two alignment items: 4.6. Federal Agency Cybersecurity Alignment and 4.7. International Aspects, Impacts, and Alignment

<u>4.6. Federal Agency Cybersecurity Alignment:</u> It is extremely important we push for alignment in these key areas. Mapping agencies' cybersecurity risks to their missions is important and should be applied government-wide In fact, we understand the White House has directed federal agencies to use the Framework. The General Services Administration (GSA) and Department of Defense (DoD), through the Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition, are developing recommendations regarding the federal

government instituting a federal acquisition cyber risk management strategy. As ITI recommended in an April 2014 filing on those agencies' work,[5] GSA/DoD should consider using this opportunity to develop 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, GSA and DoD 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.

4.7. International Aspects, Impacts, and Alignment: ITI has already discussed in much of our response above why international alignment is essential. See the response to Part I, Question 9.

- ITI is concerned about the shape of work in these areas: 4.3. Conformity Assessment, 4.8. Supply Chain Risk Management, and 4.9 Technical Privacy Standards.

4.3 Conformity Assessment: As ITI wrote in our April 2013 response[6] to NIST's first RFI as it launched work developing the Framework, it is essential that the marketplace determine when conformity assessment related to cybersecurity risk management is needed, what organizations should conduct those evaluations, and the appropriate way to manage an evaluation. This will allow the conformance assessment industry to move at a pace more closely tied to the pace at which threats develop and at which industry designs, develops and implements solutions that respond to these threats. Finally, most importantly, a global approach is key. There are standards for how to appropriately conduct conformity assessment that are based on global consensus and are globally deployed.

In addition, it is important to note the guidance on use of the Framework does not support conformity assessment per se because the tier concept is a maturity model concept that does not define a requirement to be met. An organization chooses the subcategories it believes are applicable to itself, and that selection will vary from organization to organization. It would be difficult to develop a conformity assessment methodology in these circumstances because there is no set of defined requirements to which a judgment of conformity or nonconformity can be applied.

4.8. Supply Chain Risk Management: NIST has identified supply chain risk management as an area for further development, but we caution against taking up this topic in the Framework context. First, we note that the notion of "supply chain risk management" itself is extremely broad and no consensus definition exists. Further, some international standards are under development in this area—and ITI members are already contributing to these processes, but these

[5] "ITI/ITAPS response to the request for comments from the GSA-DOD Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition (recommendation on a federal acquisition cyber risk management strategy)," submitted April 28, 2014, found at http://www.itic.org/dotAsset/bb8efe5e-09b8-43b7-8834-66c48e193d5b.pdf

[6] ITI comments in response to NIST RFI: "Developing a Framework to Improve Critical Infrastructure Cybersecurity, filed April 8, 2013, found at http://www.itic.org/dotAsset/918477ac-ce31-4900-926e-e523bac6db7a.pdf

are still nascent efforts that have not yet been implemented widely by industry. In fact, the current state of practices in supply chain risk management is characterized by significant diversity. As a result, we do not believe that this issue is ripe for being tackled within the Cybersecurity Framework, because it is unclear what such a work stream would accomplish and how it would interface with the ongoing international processes.

4.9. Technical Privacy Standards: We have some concerns about the Technical Privacy Standards work proposed by NIST. While privacy engineering can offer tremendous value, NIST's work in this area should be carefully focused. Most importantly, it should not focus on developing a framework or a technical standard. A framework or technical standard can only follow from predefined policy objectives. NIST's privacy engineering work, in its current form (including the recent September 2014 workshop and underlying materials), includes defining privacy harms and choosing among privacy engineering objectives, without the prerequisite policy references. This inevitably leads to less transparent policy-making embedded as part of a technical standards development process.

We value NIST's interest in contributing its technical expertise in the privacy realm and encourage NIST to leverage that expertise to further the privacy engineering field by focusing its efforts on cataloguing, in a policy-neutral manner, how privacy engineers accomplish various privacy-by-design or information management processes they are tasked with developing. A cataloguing effort will involve input from numerous stakeholders, including privacy engineers, as well as those within organizations that task engineers with achieving certain processes and outcomes. In particular, those in industries governed by established privacy laws would have expertise in contributing to this initiative. To provide inputs for this cataloging, organizations could share practical examples of how they establish privacy programs and how they use Privacy Impact Assessments to identify, assess, and address potential privacy issues. The cataloguing initiative will provide a better and shared understanding of the use of privacy engineering solutions in corporate data governance structures. In connection with such an initiative, to gain robust participation, it will be useful for NIST to indicate that this cataloging initiative is designed to index approaches in use, rather than yield specific endorsements or organization commitments.

We believe that this cataloging initiative will yield significant benefits in privacy protection. Such a resource will make it much easier for business and government to understand the universe of privacy protective engineering solutions currently in use, and has potential to drive further innovation in the privacy engineering field. SMBs will likely benefit in particular from such a resource.

CONCLUSION

ITI would like to again thank NIST for its commitment to partnering with the private sector to improve cybersecurity. ITI also would like to commend the Administration for having integrated so much of the input it has received from industry over the past few years on this topic, and for its willingness and eagerness to consistently engage with our companies and the ICT industry

generally on how government and industry can work together to improve cybersecurity. The commitment to industry outreach in this regard is an excellent example of the effective public-private partnerships that are essential to improving cybersecurity.

We hope that our comments will receive due consideration. We are available at any time to elaborate on our comments and our suggestions. ITI and its members look forward to continuing to work with NIST and the Administration generally to improve America's cybersecurity posture. Please continue to consider ITI a resource on cybersecurity issues moving forward.

Thank you very much for your consideration.
Sincerely,

Danielle Kriz
Director, Global Cybersecurity Policy

ATTACHMENT

Excerpt from ITI comments: "Response to Department of Commerce Cybersecurity, Innovation, and the Internet Economy Green Paper Notice of Inquiry," submitted August 18, 2011[7]

This excerpt is provided in response to the current RFI's Part II Question 9

III. Facing the Challenges of Cybersecurity: Developing Policy Recommendations for the Future

A. CREATING A NATIONALLY RECOGNIZED APPROACH TO MINIMIZING VULNERABILITIES FOR THE I3S

Policy Recommendation A3: The U.S. government should promote and accelerate both public and private sector efforts to research, develop and implement automated security and compliance.

We strongly agree that the U.S. Government has a critical role in promoting and accelerating research and development (R&D) of key cyber security technologies, including automated security and compliance. We have long encouraged the U.S. Government to increase its R&D related to security, to help identify R&D gaps and direct resources to emerging security technologies, and to support industry's R&D.

The U.S. Government also should determine if cross-border partnerships in R&D in automated security and compliance would be helpful. It is possible that some of our trading partners are also interested in pursuing R&D in this segment of cybersecurity. If so, joining forces to advance R&D will help all of us get to our goals more quickly.

One important area of automated security and compliance is related to standard naming conventions for vulnerability elements. The Common Vulnerability Reporting Format (CVRF) is a successful industry-developed standard. NIST should consider promoting CVRF for wider use.

C. EDUCATION AND RESEARCH

Policy Recommendation C1: The Department of Commerce should work across government and with the private sector to build a stronger understanding (at both the firm and at the macro-economic level) of the costs of cyber threats and the benefits of greater security to the I3S.

[7] "ITI comments: Response to Department of Commerce Cybersecurity, Innovation, and the Internet Economy Green Paper Notice of Inquiry," submitted August 18, 2011, found at http://www.itic.org/dotAsset/b84c1859-cfa6-4c1a-9145-6c5cccfd1c72.pdf

We agree with this recommendation. Currently, as the Department is aware, many entities do not invest adequate resources in cybersecurity due to a lack of useful data on the costs of cyber threats and the benefits of greater security.

Policy Recommendation C2: The Department of Commerce should support improving online security by working with partners to promote the creation and adoption of formal cybersecurity-oriented curricula in schools. The Department of Commerce should also continue to increase involvement with the private sector to facilitate cybersecurity education and research.
What new or increased efforts should the Department of Commerce undertake to facilitate cybersecurity education?

ITI wholeheartedly agrees with the need for cybersecurity-oriented curricula in schools and agrees that the Department should work with partners to promote the development and adoption of these curricula. We are very concerned that so many computer science majors (as well as engineers whose careers will likely involve work with Internet-enabled systems, such as systems, industrial, and mechanical engineers) who graduate from U.S. universities do not learn the basics of computer security and how to build security into products from the outset. This lack of consistent education and expectation for these graduates hampers industry's ability to procure, build, deploy, and maintain more secure systems and networks.

However, ITI believes it is extremely important to ensure that "cybersecurity-oriented curricula" are not simply defined as a school offering one or two security classes that computer-related majors (or other engineers, as noted above) must take. Security is not a "class." It is a mindset, and needs to be part and parcel of each class. In other words, computer-related majors must be educated that systems have to be designed, built, and delivered to be secure. Without this approach, there will not be sufficient awareness, best practices, or other security activity to secure our systems. Civil engineering education takes such an approach. Civil engineers learn structures, and every successive class implicitly relies upon and expects the student to demonstrate knowledge of sound structural engineering. If security is not embedded throughout U.S. computer science degree programs and their curricula, little will change.

We have three specific recommendations that can help to achieve the goal described above. First, accreditation bodies for universities' computer science and related (e.g., control systems) curricula should have primary responsibility for demanding that security concepts be embedded in all computer science-related classes. The Department should encourage accreditation bodies to demand such changes in these curricula. Second, the U.S. government should tie grant monies—of all kinds, not just computer related—to computer science curricula change in universities. Although this is not the purview of the Commerce Department, the Department should encourage the responsible federal agencies in this regard. Third, the Department should bring interested and knowledgeable stakeholders together to create security examples that can be included in computer science and related textbooks, and work with the Department of Education to encourage textbook publishers to incorporate security examples and sections into all computer science textbooks. Professors would then have something to teach to.

ITI has a final important point about cybersecurity education. As the Department notes on pp. 35-38 of the Green Paper, education should focus not only on improving our engineers' ability to build secure products, which is extremely important, but also on enabling people to understand user responsibility related to cybersecurity and to take appropriate action. Cyberspace's stakeholders—consumers, businesses, governments, and infrastructure owners and operators—need to know how to reduce risks to their property, reputations, and operations. However, many stakeholders are not aware of and also do not adequately utilize the range of tools available to them to do so, such as information sharing, risk management models, technology, training, and globally accepted security standards, guidelines and best practices. Raising awareness so that cyberspace's stakeholders can use these tools is critical to improving cybersecurity. Such an approach is consistent with ITI's Principle 5. We agree with the many ideas that the Department received in response to its 2010 NOI on cybersecurity and listed in the Green Paper to improve user awareness, such as further enhancing the National Initiative for Cybersecurity Education (NICE).

- **What are the specific areas on which education and research should focus?**

Our recommendation here is general. Although there is a case for some "fundamental research," too much of an emphasis on fundamental research could result in an insufficient amount of cybersecurity research with practical applications. Federal research monies should be balanced between fundamental research and practical research. In addition, industry input is vital to helping federal grant programs determine which lines of research deserve funding so that research has practical applications and is not wasteful or duplicative.

Policy Recommendation C3: In cooperation with other agencies through the Federal Networking and Information Technology Research and Development (NITRD) framework, the Department of Commerce should begin to specifically promote research and development of technologies that help protect I3S from cyber threats.

We agree. ITI also recommends that the Department seek out industry participation in developing strategies and setting priorities related the cybersecurity-related R&D. Further, the Department should promote public-private partnerships for cybersecurity R&D, particularly partnerships that include a multi-disciplinary approach involving the IT hardware, software, and networking sectors.

D. ENSURING STANDARDS AND PRACTICES ARE GLOBAL

Policy Recommendation D1: The U.S. government should continue and increase its international collaboration and cooperation activities to promote cybersecurity policies and standards, research and other efforts that are consistent with and/or influence and improve global norms and practices.

ITI strongly commends the Department for having such a strong emphasis on international collaboration and cooperation related to government promotion of cybersecurity policies and

standards. To date, the international community has lacked the collective willingness to align their approaches to cybersecurity in a manner that recognizes that this issue is no longer just a matter of Internet security, but also one of economic prosperity. The current economic landscape highlights the urgency to address this head on. U.S. leadership is critical to encouraging all governments to engage in a meaningful conversation on the need for a global approach. In absence of a global perspective, siloed U.S. Government policies or activities may result in decreased, not increased, security and disadvantages to U.S. competitiveness and innovation. We urge the Administration to continue to commit the resources and political capital needed for an effective international focus.

We believe NIST should continue to serve as the federal coordinator for international collaboration and cooperation to promote cybersecurity standards, generally accepted industry practices, and guidelines. Moreover, NIST's role as federal coordinator—both internally and externally—for the federal government's cybersecurity standards activities must be reaffirmed and strengthened. The National Technology Transfer and Advancement Act of 1995 (NTTAA) says that NIST is "to coordinate the use by Federal agencies of private sector standards, emphasizing where possible the use of standards developed by private, consensus organizations" … and "to coordinate Federal, State, and local technical standards activities and conformity assessment activities, with private sector technical standards activities and conformity assessment activities, with the goal of eliminating unnecessary duplication and complexity in the development and promulgation of conformity assessment requirements and measures."[8] There are currently a number of federal agencies involved in the development and representation of U.S. Government policy positions in international cybersecurity standards work. While all of this work is critical and the agencies' varying perspectives and expertise is important, at the end of the day to be effective this work must be coordinated interagency to ensure a common U.S. Government position that is in the best interest of U.S. industry. NIST has been assigned, and should play, that coordinating role.

Another key point we would like to make is regarding the involvement of the Department of Commerce generally in international cybersecurity policy. Currently, the dominant bureaus with cybersecurity equities are NIST, the National Telecommunications and Information Administration (NTIA), Bureau of Industry and Security (BIS), and International Trade Administration (ITA). Each plays a very unique, but very essential, function in cybersecurity policy:

- NIST: NIST develops standards and guides for securing non-national security Federal information systems. It defines minimum security requirements for federally held information and for information systems. NIST is also a primary contributor and member of the NITRD program, leading R&D in computer forensics tool testing, seamless mobility, trustworthy information systems, information security automation, combinatorial testing, next generation access control, and Internet infrastructure protection. NIST also is responsible for the National Software Reference Library, National Vulnerability Database, and Security Content Automation Protocol. NIST

[8] https://standards.gov/NTTAA/agency/index.cfm?fuseaction=documents.PL104113

identifies methods and metrics for assessing the effectiveness of security requirements; evaluates private sector security policies for potential federal agency use; and provides general cybersecurity technical support and assistance to the private sector and federal agencies.

- NTIA: Over the past two decades, NTIA, in its role as principal adviser to the President on telecommunications and information policies, has worked closely with other parts of government on broadband deployment, Internet policy development, securing the Internet namespace, and other issues.
- BIS: BIS advances U.S. national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership.
- ITA: ITA strengthens the competitiveness of U.S. industry, promotes trade and investment, and ensures fair trade through the rigorous enforcement of our trade laws and agreements. ITA works to improve the global business environment and helps U.S. organizations compete at home and abroad. ITA promotes the commercial/business angle—informed by U.S. competitiveness interests—to U.S. Government cybersecurity policies.

Given these critical roles, all of these bureaus must allocate adequate resources to engage interagency and internationally on these issues in a manner that is commensurate with their missions and equities in this arena.

The involvement of ITA is particularly critical to helping to promote global approaches related to cybersecurity standards and best practices and thus something on which we would like to elaborate. As the Department is aware, a growing number of governments are enacting cybersecurity-related[9] laws, regulations, certification systems and other requirements, covering both government and commercial markets,[10] which purport to protect national security and economic interests. In many cases, these requirements (such as forced technology transfer or technology mandates) present obstacles to U.S. companies conducting business in those markets, are often inconsistent with generally accepted norms, standards, and best practices, and in several cases may actually violate international trade obligations. Moreover, such requirements rarely provide better security and in many cases may weaken security and disrupt global commerce. Foreign governments' cybersecurity-related policies and regulations that deviate from global approaches are becoming a top trade concern of the U.S. high-tech industry. Fortunately, this importance is reflected in the growing number of Administration officials from various Departments who are aware of and devote resources to these issues.

[9] Although not an official industry definition, "cybersecurity" is used here generally to encompass policies related to cybersecurity, computer security, data security, information security, network security, encryption, cryptography, etc.

[10] Many governments, including the United States, have very stringent requirements for security technologies sold into intelligence and military networks. This comment does not focus on requirements for those systems. Instead, we focus on discriminatory and unnecessarily trade-restrictive and burdensome requirements that apply to vast swaths of non-military or intelligence government IT systems.

It is critical to our industry that ITA contributes in a substantive and proactive way to these discussions in order to bring the critical trade perspective to the debate. In fact, being able to proactively address these cybersecurity trade issues and to develop and execute on an effective, strategic trade approach is ITA's area of expertise. We wholeheartedly appreciate ITA's commitment to addressing these concerns to date; many ITA staff work on them in partnership with our industry and interagency and are making a difference. We support ITA dedicating even more country/regional expertise from its regional units, and IT industry expertise (such as on encryption or technology standards) from its industry unit, to work on these issues. ITA's technology industry expertise is particularly essential to inform Commerce's and the Administration's (including the U.S. Trade Representative's) trade priorities and positions related to global approaches to cybersecurity standards, guidelines, and best practices. Overall, ITA's strong and consistent contribution interagency and internationally on cybersecurity is essential to supporting the goals of the National Export Initiative (NEI) and helping the U.S. IT industry remain competitive, with a positive impact on U.S. jobs.

- **Are there additional ways in which the Department of Commerce can work with other federal agencies and stakeholders to better cooperate, coordinate, and promote the adoption and development of cybersecurity standards and policy internationally?**

We have the following suggestions regarding how the U.S. Government can best do this work. ITI provided many of these suggestions in our September 20, 2010 response to the Department's Cybersecurity, Innovation, and the Internet Economy Notice of Inquiry (Docket No. 100721305-0305-01).

Engage other countries early and proactively. The U.S. Government must begin dialogues with our trading partners at an early stage on the importance of promoting and using voluntary, globally accepted cybersecurity norms and practices. The past decade has seen a rising number of instances whereby foreign governments have deviated from international norms in the area of cybersecurity standards and related requirements. In nearly all cases, the U.S. Government's and U.S. industry's responses were reactive. It is much easier to convince foreign governments to promote or adhere to global norms if we make our case before these governments adopt standards and practices than if we try to change their minds on policies, regulations, and laws already in place.

Coordinate interagency. A cohesive U.S. Government policy is important to achieving both U.S. domestic and international cybersecurity goals. Although NIST should lead the U.S. Government's work in helping to promote voluntary security best practices globally, it is imperative that as many U.S. Government agencies as possible support NIST's work. Because mandated, sometimes uniquely national cybersecurity standards and related requirements cause commercial barriers for U.S. companies, the U.S. Government trade agencies (namely ITA and USTR) have a key role in promoting a global approach. At the same time, federal technical experts responsible for or involved in cybersecurity, such as in DHS, DOD, DOJ, and other agencies, can speak authoritatively about how global approaches make the information systems and infrastructure in question more, not less, secure.

ITI understands some agencies, offices, or specific staff members already work closely on an interagency basis. ITI urges this collaboration to expand to include all relevant U.S. Government agencies and technical and policy experts as needed. Further, this interagency work must be institutionalized, not ad-hoc. Technical experts can provide technical input into talking points; participate in trade negotiations, meetings, dialogues, and workshops with foreign governments; and promote global approaches in their own technical discussions with foreign counterparts. We also suggest that such an interagency body engage directly with the private sector. A variety of mechanisms exist for such engagement. ITI would welcome the opportunity to support such engagement.

Such an approach will ensure not only that best practices are promoted globally, but also that U.S. domestic actions undertaken by U.S. federal agencies are informed by, and are not in conflict with, our global advocacy efforts.

Engage at multiple levels. Discussions of the benefits of global norms and practices regarding cybersecurity should occur at all levels of government, from career- and staff-level discussions with foreign counterparts to meetings of senior leaders. This will ensure the message is relayed to foreign governments through multiple avenues.

Consider commerce/economics and national security. The U.S. Government must proactively seek dialogues with our trading partners on how to approach cybersecurity standards and generally accepted industry practices in a manner that will achieve the requisite levels of security needed to meet national security concerns while preserving interoperability, openness, and economic development. Along these lines, ITI strongly commended the White House's International Strategy for Cyberspace, released in May 2011. We feel that framework, which balances our economic goals with our diplomatic and national security priorities, is the correct path forward to help keep the U.S. competitive worldwide while also contributing directly to our long-term economic recovery.

Encourage and support private-sector engagement. Multiple international venues (for example, international security conferences, government-sponsored trade missions, standards development workshops) are available which can provide valuable opportunities for aligned, government-industry outreach and dialogue with respect to promoting global norms and practices.

Facilitate and support global public-private-sector dialogues. The U.S. Government should play a more active role in bringing together governments and industries to discuss the need for globally consistent approaches to cybersecurity standards and practices. The Commerce Department could play a useful role in helping to organize international symposia, workshops, conferences, and the like. It is particularly important that discussions not occur solely on a bilateral basis but involve government and industry representatives from multiple countries to reflect the transborder nature of these issues and need for global solutions. Efforts should be made to include stakeholders from all industries—not only vendors and suppliers of security technologies but also companies that seek to deploy global security solutions.