Information Technology Industry Council

April 8, 2013

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: "Developing a Framework to Improve Critical Infrastructure Cybersecurity"

Dear Ms. Honeycutt:

The Information Technology Industry Council (ITI) appreciates the opportunity to respond to your RFI of February 26, 2013, "Developing a Framework to Improve 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 technology 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 the President for directing NIST to lead the development of a voluntary framework, in cooperation with the private sector, to reduce cyber risks to critical infrastructure. We also appreciate NIST's commitment to partnering with the private sector to identify areas where any additional standards may be needed, to work with the private sector to create those standards and ensure they do not manifest themselves through duplicative and unnecessary controls which hamper compliance and add unnecessary costs, and to promote the use of voluntary cybersecurity standards in a consistent and repeatable manner for businesses.

We are committed to global standards because standardized security technologies, practices, and products deployed across the global digital infrastructure enable interoperability and assurance of security policies and controls, security innovation, efficient and effective use of private sector resources, and rapid response to cybersecurity challenges. Global standardization also restrains the emergence of multiple, conflicting security requirements in multiple jurisdictions, which could compromise cybersecurity.

As a trade association, we cannot answer many of the organization-specific questions in the RFI. We have copied below in bold those questions to which we are responding. In addition to answers to those questions, immediately below we offer some general comments on the NIST approach to the Framework.

General comments on NIST's approach regarding the Cybersecurity Framework

In an effort to better inform the public cybersecurity discussion, in 2011 ITI published a comprehensive set of cybersecurity principles for industry and government.[1] ITI's six principles aim to provide a useful and important lens through which any efforts to improve cybersecurity should be viewed. To be effective, efforts to enhance cybersecurity must:

- Leverage public-private partnerships and build upon existing initiatives and resource commitments;
- Reflect the borderless, interconnected, and global nature of today's cyber environment;
- Be able to adapt rapidly to emerging threats, technologies, and business models;
- Be based on effective risk management;
- Focus on raising public awareness; and
- More directly focus on bad actors and their threats.

We are pleased the Cybersecurity Framework as envisioned reflects the approaches described in our Principles. Its emphasis on promoting global, voluntary, consensus-based standards and best practices leverages industry's efforts and resource commitments and also reflects the borderless nature of cyberspace (Principles 1 and 2). Global ICT standards respond broadly to the needs of global markets, demonstrate relevance through voluntary worldwide adoption and implementation, and are products of standardization processes that are consensus-based, transparent, and industry-led with participation open to any interested party.

The fact that the Framework will be voluntary, that participating entities may choose which standards and best practices in the Framework are right for them, and that the Framework will be a "living document that allows for ongoing consultations in order to address constantly evolving risks" acknowledges that cybersecurity efforts must be flexible and based on risk management (ITI Principles 3 and 4). We assume this means that the list also will be 'living,' i.e., expanded if and when new standards are developed that are embraced by the marketplace. Finally, the overall goal of the Framework—to assist critical infrastructure sectors and other interested entities in identifying the guidance most effective in improving their security posture—comports with our Principle #5 on the importance of raising public awareness among end-users on what they can do to improve cybersecurity.

We also fully support NIST's statement that:

> The Cybersecurity Framework will incorporate existing consensus-based standards to the fullest extent possible, consistent with requirements of the National Technology Transfer and Advancement Act of 1995, and guidance provided by Office of Management and Budget Circular A-119, "Federal Participation in the Development and Use of Voluntary

[1] The IT Industry's Cybersecurity Principles for Industry and Government, found at www.itic.org.

> Consensus Standards and in Conformity Assessment Activities." Principles articulated in the Executive Office of the President memorandum M-12-08 "Principles for Federal Engagement in Standards Activities to Address National Priorities" will be followed. The Framework should also be consistent with, and support the broad policy goals of, the Administration's 2010 "National Security Strategy," 2011 "Cyberspace Policy Review," "International Strategy for Cyberspace" of May 2011 and HSPD-7 "Critical Infrastructure Identification, Prioritization, and Protection." (RFI p. 1)

Guidance provided by the NTTAA of 1995 and OMB Circular A-119 directs agencies to use voluntary consensus standards in lieu of government-unique standards except where inconsistent with law or otherwise impractical. This approach is also in line with the statement made by President Obama upon the 2009 release of the Administration's Cyberspace Policy Review: "Let me be very clear: my administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity."

Finally, we strongly agree with the direction given by the Executive Order that the Framework be "technology neutral," and we commend NIST for stating in the introduction to the RFI that the Framework should include "technology-independent standards, guidelines and best practices." This will ensure that no specific technology is wrongly consecrated as a requirement, and instead that technology providers and users focus on managing risk and selecting specific security measures, including specific technologies, among a continuously evolving panoply of competing solutions.

As NIST Undersecretary Gallagher also rightly stated in his remarks opening the April 3, 2013 Cybersecurity Framework Workshop in Washington, DC, the NIST Cybersecurity Framework "will not be seeking to tell industry how to build your products." It is indeed imperative that the Framework not create any regulation of, or requirements related to, the design, development, manufacturing, or attributes of commercial ICT products. This is a careful delineation of the appropriate scope of cybersecurity-related regulation that will preserve and promote our industry's ability to innovate, which is critical to ensuring that our industry remains globally competitive—further strengthening cybersecurity.

In addition to decreasing security, we caution against prescriptive policy or regulatory approaches because they would set a dangerous global precedent, especially as the United States has worked so hard to discourage such initiatives at global bodies such as the International Telecommunication Union (ITU). We appreciate NIST remaining vigilant on this point in its analysis of the RFI responses and as it coordinates the development of the Framework.

Section 1: Questions Regarding Cybersecurity Practices

NIST solicits information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and other management practices related to cybersecurity. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations

perceive in meeting such requirements. This will assist in NIST's goal of developing a Framework that includes and identifies common practices across sectors.

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

Page 3 of the RFI states:

> It is anticipated that the Framework will: (i) Include consideration of sustainable approaches for assessing conformity to identified standards and guidelines; (ii) assist in the selection and development of an optimal conformity assessment approach; and (iii) facilitate the implementation of selected approach(es) that could cover technology varying in scope from individual devices or components to large-scale organizational operations. The decisions on the type, independence and technical rigor of these conformity assessment approaches should be risk-based. The need for confidence in conformity must be balanced with cost to the public and private sectors, including their international operations and legal obligations. Successful conformity assessment programs provide the needed level of confidence, are efficient and have a sustainable and scalable business case.

ITI largely agrees with this statement. As you are aware, conformity assessment refers to a process used to demonstrate that a product, service, or organization meets specified requirements, such as standards. Assessing conformance is done by organizations—usually independent, private laboratories—authorized to certify, inspect and test the product, service, or organization against the specification. Conformity assessment can focus on certification/type testing, as well as management system controls (for processes).

As with standards, 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 a cross-sectoral industry such as the ICT industry (our products are used across sectors) ICT vendors may obtain sector-specific conformity assessments for products that have sector-specific uses. However, the corresponding standards do not prescribe the manner in which the products are developed, but rather what sector-specific technology features and functionalities they include.

Section 2: Use of Frameworks, Standards, Guidelines and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems

supporting organizational missions and business functions. NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations. NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage.

1. What additional approaches already exist?

Globally developed security standards form the foundation of cybersecurity risk management. However, it is important to stress that there is no one "cybersecurity standard" or set of practices that is applicable across the board. Cybersecurity risk management is complex, including many moving parts, responsible parties, and standards. In addition, the global ICT industry continually establishes new standardization efforts addressing emerging cybersecurity risk concerns.

Overall, the ICT industry uses a range of global standards. U.S. ICT companies contribute to developing such standards on a global, voluntary, and consensus-based basis through a range of organizations including formal standards development bodies as well as consortia and alliances. Examples include:

- Institute of Electrical and Electronics Engineers (IEEE)
- International Organization for Standardization (ISO)
- International Electrotechnical Commission (IEC)
- International Telecommunication Union (ITU)
- Internet Engineering Task Force (IETF)
- 3rd Generation Partnership Project (3GPP)
- World Wide Web Consortium (W3C)

Below we provide some examples of standards developed and used by our member companies. While not exhaustive, these standards illustrate a range of options used.

- ISO/IEC 15408 (Common Criteria for Information Technology Security Evaluation (CC)) is the global standard for computer security certification. The CC is based on the ISO/IEC standard and is a multi-lateral agreement – the Common Criteria Recognition Arrangement (CCRA) - among 26 countries including the United States, Japan, the United Kingdom, Australia, Germany, Korea, and India.
- The IETF efforts on security automation are critical to gaining global acceptance on protocols and data formats. These efforts include nascent work aimed to help industry manage and measure compliance, while enabling situational awareness and risk prioritization from the assessment capabilities coupled with information on assets and threat/vulnerability feeds. Other work is seeking to provide a representation for the most commonly exchanged incident and indicator information, using a set of IETF protocols to enable common interfaces for the exchanges. Other work is on ways to assess systems prior to joining the network to ensure endpoint compliance.

- 3GPP has begun to address the issue of security assurance standards and has chartered its security group, SA3, to develop a suitable methodology for mobile network security assurance. This work is still in progress, but is moving towards re-using Common Criteria methodology to define appropriate security assurance criteria for mobile networks. Once a security methodology is agreed upon, SA3 will likely begin work to produce a collaborative Protection Profile (cPP) that would be used for security compliance of mobile networks.

In general, we prefer frameworks that place emphasis on risk management, governance, and good ICT service management, and that allow individual companies to adjust and refine the security and control objectives and implementations based on our business methods, technology architectures, and risk management approach. As an example, ISO standards are particularly helpful because they offer methodological approaches to assessing and managing risk, rather than prescriptive responses or technical solutions. One of the seminal risk management standards is the ISO 27000 series. This is a security control framework that provides a globally recognized baseline set of control objectives and controls statements with supporting guidelines and risk management framework to provide conformity among organizations' security policies. As security automation improves, control frameworks can be used to manage security requirements and reporting across and between organizations. This combination of consistent reporting on automated controls will only increase in importance.

On the other hand, we find that approaches that prescribe specific technical implementations to apply controls might not make good business sense based on the business scenario and the risk profile of the business and technology activities.

We urge NIST to promote the adoption of existing frameworks that are:

- Based on a risk management approach;
- Based on analysis of real-world data and experience to identify control objectives and guidelines that have been shown to be effective at addressing risk; and
- Presented and composed with a business-oriented audience in mind, with notes or appendices to deliver security and technology domain-specific details.

9. What other outreach would be helpful?

Outreach regarding the Framework should be domestic as well as global.

Domestically, as the U.S. Government seeks to inform stakeholders about the Framework, one path it should take is to build on its existing sponsorship of the private sector-created and led National Cyber Security Alliance (www.staysafeoline.org), which is the leading security awareness public-private partnership in existence.

Although we hope that other governments around the world emulate NIST's approach and Framework (see our answer to Section 3, question 10 below), there is a risk in developing this Framework. Some governments might misunderstand the role of the Framework and incorrectly interpret its development as a sign that country-specific, regulatory action is both necessary and warranted. As ITI has talked to other governments since the release of the Executive Order, we

have carefully stressed that, although NIST does develop cybersecurity standards for U.S. federal non-national security computer systems (standards that are then mandated for federal agency use by the Office of Management and Budget (OMB)), in this Framework NIST is NOT developing standards that will be mandated on industry. This is a nuance that could be easily lost. Further, the development of the Framework will be an industry-led endeavor. The U.S. Government should conduct extensive global outreach to educate other governments about the development, purpose and role of the Framework—what it is and what it is not—and encourage those governments to take similar approaches based on voluntary, global, industry-led standards.

Section 3: Specific Industry Approaches

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry. NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- ***Separation of business from operational systems;***
- ***Use of encryption and key management;***
- ***Identification and authorization of users accessing systems;***
- ***Asset identification and management;***
- ***Monitoring and incident detection tools and capabilities;***
- ***Incident handling policies and procedures;***
- ***Mission/system resiliency practices;***
- ***Security engineering practices;***
- ***Privacy and civil liberties protection***

4. Are some of these practices not applicable for business or mission needs within particular sectors?

While some of the ICT sector's products are sector-specific (i.e. an ICT solution developed specifically for the management of a power generation system), most are not. The same databases, routers or processors are used by companies in the public, retail, defense, power, transportation, tourism, and other sectors. Whether its products are sector-specific or not, a commercial-off-the-shelf (COTS) ICT vendor will generally use the same design, development and manufacturing processes and practices. Therefore, these products do not comply with different and divergent product assurance standards. Instead, they comply with and are evaluated under cross-sectoral product assurance standards. That is not to say that ICT vendors do not obtain sector-specific conformity assessments for products that have sector-specific uses. However, the corresponding standards do not prescribe the manner in which the products are developed, but rather what sector-specific technology features and functionalities they include.

10. What are the international implications of this framework on your global business or in policymaking in other countries?

ITI's 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

international policies on security innovation and the need for governments' policies to be globally compatible. Cybersecurity approaches that differ dramatically by country—a policy patchwork—not only present potentially negative consequences for security, but also disrupt global commerce and ignore the borderless nature of the Internet.

We hope this Framework will lead to greater global consensus for government cybersecurity policymaking and sends a signal to our trading partners about the most appropriate way to improve cybersecurity. To achieve a global consensus, it would be helpful if the United States were to solicit comments and support from other countries during development of the Framework. Further, it is important that the U.S. Government set a positive example regarding the essential role that the global standards play for both industry and government. The explicit reference in the RFI that any consensus-based standards also be *global* reflects the realities of cyberspace and the ICT marketplace, will facilitate global deployment of security measures, and will reduce barriers to trade.

This Framework will perhaps be emulated by other governments around the world in their policy environments. We would support them doing so, because it would create consistent and cohesive approaches across geographies as well as a commitment to the global standardization process, public-private partnerships, and a voluntary—as opposed to regulatory--approach. Thus, the U.S. Government has a strong responsibility to make sure any Framework we develop would be equally beneficial if deployed globally.

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 responses to the important questions raised in the RFI are helpful and 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