ADVANCING GLOBAL COMMUNICATIONS
TIAONLINE.ORG

April 8, 2013

Via Electronic Filing (cyberframework@nist.gov)

Diane Honeycutt,
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Re: Comments of the Telecommunications Industry Association to the National Institute of Standards and Technology on *Developing a Framework To Improve Critical Infrastructure Cybersecurity* (Docket Number 130208119–3119–01)

I. Introduction and Statement of Interest

The Telecommunications Industry Association ("TIA") hereby submits comment on the National Institute of Standards & Technology's ("NIST") request for information to inform its effort to develop a framework to reduce cyber risks to critical infrastructure.[1] We appreciate that NIST must strike a delicate balance of numerous interests in the development of the Cybersecurity Framework. Below, in our responses to the questions posed by NIST in the RFI, we urge that NIST proceed in its implementation of the EO guided by the following principles: (1) that successful efforts to improve cybersecurity will leverage public-private partnerships to effectively collaborate on addressing current and emerging threats; (2) that the U.S. government should enable and stimulate greater cyber threat information sharing between the public and private sector; (3) that policymakers and regulators should ensure that they address economic barriers for owners and operators of critical infrastructure in efforts to secure cyberspace; (4) that Federal research funding for ICT and specifically cybersecurity research and development should be prioritized; (5) that the global nature of the information and communications

[1] National Institute of Standards and Technology, *Developing a Framework to Improve Critical Infrastructure Cybersecurity*, Notice and Request for Information, 78 Fed. Reg. 13024 (Feb. 26, 2013) ("RFI"); Executive Order – Improving Critical Infrastructure Cybersecurity, rel. Feb. 12, 2013 ("EO").

technology ("ICT") industry necessarily requires a global approach to address cybersecurity concerns; and (6) that a global supply chain can only be secured through an industry-driven adoption of best practices and global standards.

TIA represents approximately 500 ICT manufacturer, vendor, and supplier companies and organizations in standards, government affairs, and market intelligence. Numerous TIA members are companies producing ICT products and systems, creating information security-related technologies, and providing ICT services information systems, or components of information systems. These products and services innovatively serve many of the sectors directly impacted by the EO and the related Presidential Policy Directive.[2] Representing our membership's commitments in this area, we hold membership and are actively engaged in key public-private efforts that contribute to secure information systems, including the Communications Sector Coordinating Council (CSCC)[3] and the Federal Communications Commission's ("FCC") Communications Security, Reliability and Interoperability Council ("CSRIC").[4] TIA also actively convenes its members to address issues related to the EO and PPD-21 in its Cybersecurity Working Group, and has recently released cybersecurity policy recommendations for critical infrastructure and the global supply chain that have shaped our views below, and that we urge NIST to review.[5]

---

[2] Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience, rel. Feb. 12, 2013 ("PPD 21").

[3] *See* http://www.commscc.org/.

[4] *See* http://transition.fcc.gov/pshs/advisory/csric/.

[5] TIA, *Securing the Network: Cybersecurity Recommendations for Critical Infrastructure and the Global Supply Chain* (Jul. 2012), *available at* http://www.tiaonline.org/sites/default/files/pages/TIA%20Cybersecurity%20White%20Paper-Critical%20Infrastructure%20%26%20Global%20Supply%20Chain_0.pdf#overlay-context=policy/white-papers (TIA Cybersecurity Whitepaper).

In addition, a major function of TIA is the writing and maintenance of voluntary industry standards and specifications, as well as the formulation of technical positions for presentation on behalf of the United States in certain international standards fora. TIA is accredited by American National Standards Institute (ANSI) to develop voluntary industry standards for a wide variety of telecommunications products and sponsors more than 70 standards formulating committees. These committees are made up of over 1,000 volunteer participants, including representatives from manufacturers of telecommunications equipment, service providers and end-users, including the United States government. The member companies and other stakeholders participating in the efforts of these committees and sub-groups have produced more than 3,000 standards and technical papers that are used by companies and governments to produce interoperable products around the world.[6]

TIA's standards development activities have both a national and global reach and impact. TIA is one of the founding partners, and also serves as Secretariat for 3GPP2 (a consortium of five SSOs in the U.S., Japan, Korea, and China with more than 65 member companies) which is engaged in drafting future-oriented wireless communications standards.[7] TIA also is active in the formulation of United States positions on technical and policy issues, administering four International Secretariats and 16 U.S. Technical Advisory Groups (TAGs) to international technical standards committees at the International Electrotechnical Commission (IEC). Finally, TIA is a founding member of the oneM2M, an international partnership that is working to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide.[8]

---

[6] TIA publishes an annual report that includes the latest actions taken by each respective TIA engineering committee toward the development of standards for the advancement of global communications. *See* TIA, Standards & Technology Annual Report (2012), *available at* http://www.tiaonline.org/standards_/about/documents/STAR_2012_Web.pdf. TIA standards are available from IHS, Inc. *See* http://www.ihs.com/.

[7] *See* http://www.3gpp2.org/Public_html/Misc/AboutHome.cfm.

[8] *See* http://onem2m.org/.

II. TIA Responses to Questions Posed in the NIST Request for Information

Current Risk Management Practices

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

Public-private partnerships. TIA believes that efforts to improve cybersecurity should leverage public-private partnerships as an effective tool for collaboration on addressing current and emerging threats. Public-private partnerships have been recognized as the basis for the cyber defense of critical infrastructure and cybersecurity policy for the last decade.[9] The success of critical infrastructure owners and operators in preventing progressively complicated attacks has stemmed from the voluntary, public-private model in use because this model is able to evolve in response to changes in threats to critical infrastructure and the risk environment. As both the complexity and number of attacks grow, it will be critical that NIST and other United States government agencies leverage and augment existing public-private partnerships. TIA members believe that transitioning from a public-private partnership model to a mandatory regulatory regime, or one that is effectively of a mandatory nature, would have a negative impact on the security of critical infrastructure. We note that the National Infrastructure Protection Plan ("NIPP"), which has formalized the public-private partnerships in the 18 critical infrastructure sectors with Sector Specific Plans and Sector Coordinating Councils ("SCCs") describes the benefits of the public-private partnership as follows:

> The multidimensional public-private sector partnership is the key to success in this inherently complex mission area. *** [It] has facilitated closer cooperation and a trusted relationship in and across the 18 CIKR sectors. *** Integrating multi-jurisdictional and multi-sector authorities, capabilities, and resources in a unified but flexible approach that

[9] Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, 18 (2009) *available at* www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

> can also be tailored to specific sector and regional risk landscapes and operating environments is the path to successfully enhancing our Nation's CIKR protection.
>
> Implementation of the NIPP is coordinated among CIKR partners to ensure that it does not result in the creation of duplicative or costly risk management requirements that offer little enhancement of CIKR protection. *** The NIPP provides the framework for the unprecedented cooperation that is needed to develop, implement, and maintain a coordinated national effort to bring together government at all levels, the private sector, nongovernmental organizations, and international partners.[10]

TIA strongly believes that the public-private partnership model for cybersecurity achieves what mandatory requirements cannot: (1) collaboration and cooperation instead of compliance in lieu of penalty; (2) an elastic and cohesive method to confront cyber attacks; and (3) prevention of duplicative and expensive requirements, permitting assets to be concentrated on protection rather than outmoded mandates.

Between the NIPP and many other efforts, there are numerous public-private partnerships that can be utilized and enhanced to safeguard critical infrastructure, including the National Coordination Center/Communications Information Sharing and Analysis Center ("NCS/ISAC"), the National Cybersecurity and Communications Integration Center ("NCCIC"), the Partnership for Critical Infrastructure Security ("PCIS"), the Control Systems Security Program ("CSSP"), the Communications Coordinating Council, the IT Coordinating Council, the Network Security Information Exchange, the Cross-Sector Cyber Security Working Group ("CSCSWG"), the FCC's CSRIC, and the National Security Telecommunications Advisory Committee ("NSTAC"). These and other public-private partnerships should serve as the foundation for moving forward with critical infrastructure protection.

---

[10] National Infrastructure Protection Plan, i-8 (2009) *available at* www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

Based on the above, TIA recommends that in its development of the Framework, NIST should concentrate its efforts on improving public-private partnerships, as they have demonstrated themselves as effective means in giving industry required flexibility to prevent attacks, and to specifically avoid effectually constructing a new regulatory regime.

Information sharing. Lacking the capability to efficiently share crucial and timely cybersecurity data and information while ensuring strong privacy protections is certainly one of the greatest challenges to improving cybersecurity practices across critical infrastructure. TIA encourages NIST and other Federal actors to eliminate major obstacles to information sharing and to facilitate cooperation in defense against cyber attacks. For example, TIA has supported the Cyber Intelligence Sharing Protection Act (H.R. 3523), while appreciating efforts to ensure that an information sharing regime appropriately addresses privacy and civil liberties concerns.[11] While the Department of Homeland Security ("DHS") has a number of responsibilities under the Executive Order to enhance information sharing, we believe that the Framework should complement the enhancements made to the information sharing regime by DHS.

Maintaining parity with Federal Information Security Management Act implementation. TIA supports efforts to improve and harmonize cybersecurity programs across government agencies. In doing so, TIA has urged policymakers to focus on the security practices of agencies and their personnel – people and processes – while avoiding ICT security requirements that could prove disruptive to the ICT supply chain. Consistent with our views that economic barriers for owners and operators of critical infrastructure is a crucial step in securing cyberspace,[12] we urge NIST to ensure that any improvements to security and privacy requirements that it places on the private sector in the Framework is not inconsistent with FISMA implementation requirements on agencies.[13] We believe that NIST's FISMA implementations generally reflect

---

[11] See Letter from Grant Sieffert, President, TIA, to U.S. House of Representatives Leadership (Apr. 18, 2012), *available at* http://www.tiaonline.org/sites/default/files/pages/TIA_Letter_to_Speaker_Boehner_and_Leader_Pelos_4_18_12.pdf

[12] TIA Cybersecurity Whitepaper at 5-6.

[13] Federal Information Security Management Act ("FISMA"), Public Law 107-347; Office of Management and Budget (OMB) Circular A-130.

that the ICT industry is already working collaboratively to address information security concerns, and that the inclusion of these efforts will enable as efficient an implementation as possible for the U.S. Government in its continued effort to protect Federal information systems, along with the realization of the Framework.

Insufficient cybersecurity research and development. While the United States maintains the most resilient research ecosystem across the globe, indications are emerging of wearing away in the ICT sector as other countries continue to make decisive measures to interest investment in ICT research to build innovation-based economies.[14] The resulting effects on the U.S. ICT sector of a less competitive ICT research ecosystem are tangible. As far back as 2009, the National Academy of Sciences stated that "[t]he nation risks ceding IT leadership to other generations within a generation unless the United States recommits itself to providing the resources needed to fuel U.S. IT innovation."[15] TIA maintains that the United States government has not offered or effected the commitment needed to avert this risk: Federal investment in ICT research remains comparatively low when compared to other scientific fields. TIA believes that Federal funding for cybersecurity research and development should be prioritized, and should coordinate research activities amongst contributing agencies, incorporating industry input.

Past the economic costs of other nations bettering the United States in ICT research and development, the most distressing are in the area of national security. We note that this risk is evident to the United States government – the National Critical Infrastructure Security and Resilience R&D Plan emphasize the changing nature of threats, annual metrics, and other appropriate data being used to ascertain priorities and to help point R&D requirements and investments in the right direction.[16]

---

[14] TIA, *U.S. ICT R&D Policy Report*, (2011) *available at* http://www.tiaonline.org/sites/default/files/pages/TIA%20U%20S%20%20ICT%20RD%20Policy%20Report.pdf.

[15] NRC, *Assessing the Impacts of Changes in the Information Technology R&D Ecosystem: Retaining Leadership in an Increasingly Global Environment*, 1 (2009), *available at* www.nap.edu/catalog/12174.html.

[16] DHS, National Infrastructure Protection Plan (2009), *available at* http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

Poor public awareness and education. It is well-documented that a large majority of successful cybersecurity attacks can be prevented through better cyber "hygiene." TIA strongly supports Federal efforts to increase awareness of cybersecurity issues among both institutional users and the general public.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

Maintaining the flexibility and the ability to innovate. When forming recommendations that are intended to move across sectors, the danger inherently exists to overgeneralize in recommendations. TIA believes that where recommendations in the Framework do cross sectors, an utmost concern for NIST must be to allow specific sectors to continue to innovate to address specific threats. We believe that this will be a challenge that can be worked out through a transparent and inclusive process overseen by NIST.

Currently, "critical infrastructure" sectors affected by the EO include energy, agriculture/food, information technology, banking/finance, telecommunications/broadcasting, commercial services, defense industrial base, chemical, dams, health care, water, nuclear, critical manufacturing, transportation; and postal/shipping. These sectors have been identified by DHS pursuant to Presidential Policy Directive #7, which established US cybersecurity policy in 2003.[17]

Under the EO, not later than July 12, 2013, the Secretary of Homeland Security ("Secretary") shall identify critical infrastructure where a cybersecurity incident could result in catastrophic regional or national effects on public health or safety, economic security, or national security, using a consultative process and drawing on the expertise of the Sector Specific Agencies ("SSAs") designated in PPD-21, which accompanied the release of the EO. Per the EO, DHS is the SSA for communications. The EO, however, prohibits, the Secretary from identifying "any

[17] Presidential Policy Directive/PPD-7, National Terrorism Advisory System (NTAS), rel. Jan. 16, 2011.

commercial information technology products or consumer information technology services" under this process. TIA supports the inclusion of this crucial prohibition that will help ensure that the manufacturers and suppliers of such commercial information technology products have the needed flexibility to innovate. So long as DHS, in fulfilling its responsibilities surrounding the identification of critical infrastructure, does not stifle the ability of the manufacturers of the ICT equipment that enables each of the critical infrastructure sectors to innovate, and instead relies on each sector member to determine their needs through the ICT they comprise their service of, we believe that the Framework can embody the necessary flexibility for effective cybersecurity across sectors. TIA urges NIST, in developing the Framework and in other efforts to implement the EO, reflect this important need.

The necessity of international approaches and standards. TIA urges NIST to ensure that the Framework reflects the priority for U.S.-based technologies' continued success in the global marketplace which has been enabled through the development of internationally-used standards and best practices. Consistent with this theme, we urge NIST to recognize that that the global nature of the ICT industry necessarily requires a global approach to address cybersecurity concerns, and that a global supply chain can only be secured through an industry-driven adoption of best practices and global standards. ICT products are often designed and built in different locations using globally-sourced components, making it very difficult to classify specific products as U.S. or non-U.S. products. Aside from the complexity in defining the nationality of a particular product, ICT companies conduct different functions (manufacturing, R&D and services) across facilities in multiple different countries, often making it difficult to classify companies as U.S. or non-U.S. companies. To stay competitive, ICT companies need to continue to use a distributed approach to their technology development and manufacturing. For example, TIA standards are used throughout the world across a number of technologies, as well as other areas such as building codes. To this end, NIST's efforts in this area should incorporate other Federal agencies' efforts as well as North American SDOs and companies to ensure that any standards, regardless of where they are developed, be viewed as "international" standards if they are globally adopted.

Any approach taken in the Framework must involve international cooperation and heavy engagement with the private sector but should not include language that might put the government in a position to determine the future design and development of technology. TIA believes that the United States should work with other governments to establish international security standards in order to prevent hobbling United States industry with United States-only standards. We are concerned about the impact on our nation's global competiveness as well as technology innovation and development of having the United States government set specific technical standards. Neither the Framework nor any other government action should enact cybersecurity policies that would restrict trade in telecommunications equipment imported to, or exported from, other countries that are part of the global trading system. While other countries cite similar concerns regarding foreign ICT equipment and are currently considering trade restrictive measures, we believe that the U.S. should be a leader is this area: TIA recommends that the U.S. government exercise extreme caution in how it approaches this issue since U.S. policy will effectively serve as a global standard. If the U.S. develops unique approaches that have the effect of restricting trade unnecessarily, U.S. global economic competitiveness could be severely affected by other export markets adopting similar restrictive policies. In short, a global industry necessarily requires a global approach to address cybersecurity concerns.

Incorporating best practices. TIA believes that the use of non-mandatory best practices has resulted in immeasurable increases in communications network resiliency and security, along with supply chain integrity. In practice, best practices are not "created," but are recognized by stakeholders through information sharing activities as already widely-used effective means to address issues. Given the fact that each best practice is not relevant for each area, sector, node, etc. of the communications industry, because they are not mandated, network operators are allowed for the flexibility to employ the best equipment and systems that meets their specific challenges to network reliability. In addition, best practices allow for the "co-existence of new and old technologies"[18] and therefore help facilitate the smoothest transitions in technology deployments. There are currently numerous voluntary industry efforts underway that continually

[18] CSRIC Working Group 6, *Final Report: Best Practices Implementation* (rel. Dec. 2010) at 3.

formulate, aggregate, and update best practices, and network operators and equipment vendors regularly look to best practices, both internal and external to their organization, notably the FCC CSRIC's Cyber Security Best Practices Working Group.[19] We strongly urge NIST to incorporate the importance of best practices into the Framework, and use the Framework to promote the development of further best practices within, and where appropriate, across sectors.

Defining gaps in the development of the Framework. While TIA believes along with others that the communications sector will prove to be a more developed area in this examination by NIST, inevitably gaps will be found both within and across sectors, and a need may be identified for important new standards development. We urge NIST to respect and encourage ongoing standards development efforts may address such gaps. The communications sector does this currently, and we believe that it can serve as a model for other sectors.

Maintaining parity with FISMA implementation. For the same reasons listed under this subheading under Question 1 above, we believe that NIST must ensure that the Framework is less prescriptive or at most consistent with FISMA implementation requirements on agencies.

Establishing an open and inclusive procedure, and ensuring fairness. In developing the Framework, NIST will need to ensure that its process is transparent and inclusive. Because it is required by the Executive Order and based on NIST's past administration of inclusive and consensus-based processes, such as in the development of FISMA implementation documents, this is not necessarily one of NIST's greatest challenges in developing the cross-sector framework, but we do wish to emphasize its importance and suggest that NIST could ensure this challenge is met by publicly posting all comments received in the development of the Framework. TIA supports that the Framework promote transparency, fairness, and disclosure of conflicts of interest as essential characteristics of the conformity assessment process. We believe

[19] We note that the CSRIC has specifically addressed cybersecurity best practices, including those which address general "hygiene," and a recommended approach to cyber attacks, amongst many others which the Framework should incorporate. *See* CSRIC Working Group 2A, *Cyber Security Best Practices, Final Report*, (Mar. 2011), *available at* http://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf..

that this important inclusion will add a heightened level of trust amongst those involved in the process and will increase competition.

3. Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?

ICT manufacturers and vendors understand that no network, no matter the planning or regulation, can be designed and implemented to withstand every possible source of failure.[20] We also recognize that, in spite of network evolution and development of innovative applications and services, legacy infrastructure is, and will continue to be, a critical aspect of secure communications networks as technology continues to transition to IP-based delivery systems.[21] However, we note that despite this reality, today's networks, including legacy wireline systems, are continually evolving to meet emerging challenges to security with success.

The degree of reliance and security expected by Americans on communications networks would not be to the degree that it currently is if networks were not resilient or reliable. Whether a network consists primarily of legacy technology or evolved technology (or some combination of the two), network operators and their vendor suppliers have and will continue to require a high degree of flexibility to make decisions to improve network security based on unique circumstances and available resources. These organizations routinely make hyper-local decisions on how to address security challenges based on direct knowledge of unique threats and priorities

[20] *See* NSTAC 2011 Report at 1 ("While it would be near impossible to develop and maintain networks that are invulnerable to disruption, ensuring long-term communications resilience requires that the Government understand future systems and the future technology landscape when investing in and planning for durable, survivable communications for Government officials, first responders, and the general population.").

[21] "For many years the NS/EP community has relied extensively on public telecommunications networks for a large portion of its NS/EP communications needs. This reliance has increased in recent years as the functionality of public networks has improved and as the Federal Government has found more efficient and effective ways to use public telecommunications services. As public network providers have deployed more advanced equipment, the increased use of public telecommunications networks has often also brought the benefits of new features at substantially more cost-effective rates to the Federal Government. Communications Security, Reliability and Interoperability Council (CSRIC) Working Group 7, *Final Report: Planning for NS/EP Next Generation Network Priority Services during Pandemic Events* (rel. Dec. 2010) at 14 (CSRIC WG7 2010 Report).

guided by already-existing industry standards and best practices. All the while, these critical decisions are balanced with the availability of investment capital.

Regarding how senior management communicates and oversees these policies and procedures, we note for NIST that TIA consists of approximately 500 companies that drastically range in numerous ways, including market, degree of security required in products, and size, making this question difficult to answer. It is most appropriate for individual organizations to answer this question specific to their own senior management practices.

4. Where do organizations locate their cybersecurity risk management program/office?

We believe that it is most appropriate for individual organizations to answer this question specific to their own practices.

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

ICT manufacturers and vendors who enable each critical infrastructure sector to function and to communicate with other entities. In that context, defining and assessing risks generally and for the purposes of cybersecurity is a unique evaluation that considers numerous factors that may help or hurt the network, including software, hardware, human, and inter-government relationship factors.[22] Other important factors include those noted in the 20 Critical Controls,[23] all of which were recently determined by the FCC's CSRIC to be applicable to the enterprise communications networks.[24]

---

[22] *See* NSTAC, *Next Generation Networks Task Force Report* (rel. Mar. 28, 2006) at G-1 to G-10.

[23] *See* http://www.sans.org/critical-security-controls/.

[24] *See* CSRIC Working Group 11, *Consensus Cyber Security Controls, Final Report*, (Mar. 2013) at Appendix 6, *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG11_Report_March_%202013.pdf.

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

Effective protection of enterprise systems is a necessary ingredient of effective protection of network operations, and is required to remain competitive in the manufacturing and vending of ICT. In this way, product security informs most if not all aspects of enterprise risk management. TIA members work with their network operator customers to ensure that cybersecurity risks are adequately incorporated into enterprise risk management. To what degree does vary on the needs of the customer; however, more and more, cybersecurity concerns are of increasing importance to operators. We note that unsecured enterprise systems are a principal attack vector through which Internet service provider ("ISP") and carrier network operations are attacked because ISPs are frequently connected to unsecured enterprise systems and have widely known and widely exploited vulnerabilities.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

The communications sector is far ahead of others in efforts to improve the resilience of our Nation's critical infrastructure. Numerous standards, guidelines, best practices, and tools are used by ICT manufacturers and the owners & operators of telecommunications networks to understand, measure, and manage risk at the management, operational, and technical levels. TIA has aggregated an alphabetized list of these efforts, which we emphasize to be non-exclusive, that can be viewed below:

Name of SDO/Consortia/Fora	Description
3rd Generation Partnership Project (3GPP) / 3rd Generation Partnership Project 2 (3GPP2)	3GPP Security Assurance Working Group 3 (SA3) addresses security in 3GPP systems, including security and privacy requirements, security architectures and protocols and cryptographic algorithms (see http://www.3gpp.org/SA3-Security). 3GPP2 focuses specifically on cdma2000 technology (see http://www.3gpp2.org/).

Name of SDO/Consortia/Fora	Description
American National Standards Institute	ANSI-accredited standards developers, which include TIA, are working to define a suite of standards supporting national cybersecurity workforce training and professional development (see http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=2975#.UEodLI2PXTo); and financial management cybersecurity risks (see http://webstore.ansi.org/cybersecurity.aspx#.UEoc2Y2PXTo). In addition, ANSI's Homeland Security Standards Panel (ANSI-HSSP) is meeting in mid-September 2012 to examine the current landscape as well as standardization needs and solutions for global supply chain security in the U.S., Europe, and regionally (see http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=3294#.UEo9l42PXTo).
Asia-Pacific Economic Cooperation ("APEC") Security and Prosperity Steering Group ("SPSG")	The APEC's SPSG coordinates its members' cybersecurity work, and APEC leaders have committed to enacting comprehensive cybercrime laws (see http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information/Security-and-Prosperity-Steering-Group.aspx)
Cloud Security Alliance ("CSA")	CSA develops baselines for secure cloud operations covering both cloud providers and tenants (see https://cloudsecurityalliance.org/research/security-guidance/).
Common Criteria Recognition Arrangement ("CCRA")	CCRA aims to ensure that evaluations of information technology products and protection profiles are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and profiles; and to improve the availability of evaluated, security-enhanced IT products and protection profiles (see http://www.commoncriteriaportal.org/). They have produced the Common Criteria for Information Technology Security Evaluation (ISO 15408, known as CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) (see http://www.commoncriteriaportal.org/cc/).
Council of Europe	Guidelines for cooperation between law enforcement agencies and ISPs in 2008, and assists countries with implementation (see http://www.coe.int/t/informationsociety/documents/Guidelines_cooplaw_ISP_en.pdf).
European Committee for Standardization ("CEN") Cybersecurity Coordination Group ("CSCG")	CEN's CSCG acts as an advisory and coordination body to the CEN Technical Board on political and strategic matters related to cybersecurity standardization (see http://www.cen.eu/cen/Sectors/Sectors/Security%20and%20Defence/Security/Pages/CyberSecurityCoordinationGroup.aspx).
European Telecommunications Standards Institute ("ETSI")	ETIS has standards work in next generation networks, cloud, etc. (see http://webapp.etsi.org/workprogram/SimpleSearch/QueryForm.asp to search).
Institute of Electrical and Electronics Engineers ("IEEE")	IEEE has developed a number of standards in the cybersecurity realm (see http://ieeexplore.ieee.org/Xplore/guesthome.jsp#).
International Organization for Standardization ("ISO")/International Electrotechnical Commission ("IEC")	For example, the ISO/IEC 27000-series provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system (see http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42509).

Name of SDO/Consortia/Fora	Description
International Security Forum ("ISF")	The ISF develops best practices for information security, most recently updated in 2011 (see https://www.securityforum.org/downloadresearch/publicdownload2011sogp/).
Internet Engineering Task Force ("IETF")	The IETF has numerous efforts in internet security, including Application Bridging for Federated Access Beyond web, DNS-based Authentication of Named Entities, EAP Method Update, Handover Keying, IP Security Maintenance and Extensions, Kitten (GSS-API Next Generation), Kerberos, Network Endpoint Assessment, Open Authentication, Public-Key Infrastructure (X.509), and Transport Layer Security (see http://trac.tools.ietf.org/area/sec/trac/wiki). For example, RFC 2196 provides information security including network security, incident response, or security policies (see http://tools.ietf.org/html/rfc2196).
Internet Governance Forum ("IGF")	Already supports the United Nations Secretary-General in carrying out the mandate from the World Summit on the Information Society (WSIS) (Paragraph 72 of the Tunis Agenda) with regard to convening a forum for multi-stakeholder policy dialogue (see http://www.intgovforum.org/cms/) – includes regional- and country-based "Initiatives."
Open Group Trusted Technology Forum ("OTTF")	OTTF has developed a global supply chain integrity program and framework in order to provide buyers of IT products with a choice of accredited technology partners and vendors (see http://www.opengroup.org/ogttf/).
Software Assurance Forum for Excellence in Code ("SAFECode")	SAFECode develops guidance in information and communications technology products and services through the advancement of effective software assurance methods (http://www.safecode.org/index.php).
Telecommunications Industry Association	TIA develops standards across subsectors of the ICT industry, the majority of which consider security aspects as part of their development under the ANSI process. Please see below for a separate table of TIA standards that we put forward for NIST's consideration in its development of the Framework.

TIA has undertaken an effort to determine its standards activities that support cybersecurity and supply chain integrity and are directly relevant to NIST's efforts in this matter, which can contribute to an evaluation of gaps in standards and other areas that have potential needs for security and/or privacy. The various TIA committees[25] considered include TR-42 Telecommunications Cabling Systems, TR-45 Mobile and Personal Communications Systems Standards, TR-48 Vehicular Telematics, TR-49 Healthcare ICT, TR-50 Smart Device Communications, and TR-51 Smart Utility Networks. This non-exclusive list of standards, with explanations of applicability, can be viewed below:

[25] TIA publishes an annual report that includes the latest actions taken by each respective TIA engineering committee toward the development of standards for the advancement of global communications. *See* TIA, Standards & Technology Annual Report (2012), *available at* http://www.tiaonline.org/standards_/about/documents/STAR_2012_Web.pdf.

Title of Standard	Description of Standard	Importance of Standard
TIA-1121.005 Security Functions for Ultra Mobile Broadband (UMB) Air Interface Specification	This standard was prepared by Technical Specification Group C of the Third Generation Partnership Project 2 (3GPP2). This Standard is the Security Functions part of the Ultra Mobile Broadband™ (UMB™) air interface.	This standard provides a specification for securing land mobile wireless systems based upon cellular principles. This Standard is one part of the IMT-2000 CDMA Multi-Carrier, IMT-2000 CDMA MC, also known as cdma2000®
TIA-1008 ANNEX B-IPoS Security	This document is an annex to the IP over Satellite (IPoS) MAC/SLC Layer Specification that describes the security procedures supported within IPoS.	The purpose of this standard is preventing the unauthorized access to IPoS services.
Technical Standards Bulletin Smart Device Communications; Security Bulletin	This TSB addresses the management of cyber security related risk derived from or associated with the operation and use of information technology and systems and/or the environments in which they operate. The bulletin is not intended to replace or subsume other risk-related activities, programs, processes, or approaches that organizations have implemented or intend to implement addressing areas of risk management covered by other legislation, regulation, policies, programmatic initiatives, or mission and business requirements.	Machine-to-Machine ("M2M") devices are typically resource constrained devices that often have little added capacity for security. This document considers the overall security of the M2M architecture, including Data in Transit and Data at Rest. This document defines an "attack surface" with the emphasis on the possible threats against the TIA M2M architecture (TIA-4940.005). It also defines a risk model, and a method to calculate a risk vale by applying an annualized los expectancy value to illustrate the financial impact that risk decisions create.
TIA-4940.005 Smart Device Communications Reference Architecture	This document is a member of a multi-part standard that, when taken in total, defines the requirements for communications pertaining to the access agnostic (e.g. PHY and MAC agnostic) monitoring and bi-directional communication of events and information between smart devices and other devices, applications and networks.	This standard provides a high level system architecture for Machine-to-Machine (M2M) smart device communication. The architecture includes the incorporation of various security considerations, including authentication, authorization, and the use of secure protocol types.
TIA-4940.020 Smart Device Communications; Protocol Aspects; Introduction	This document is a member of a multi-part standard that, when taken in total, defines the requirements for communications pertaining to the access agnostic (e.g. PHY and MAC agnostic) monitoring and bi-directional communication of events and information between smart devices and other devices, applications and networks. This document provides an introduction to the protocols.	This standard provides the basic commands and security commands as part of the TIA Machine-to-Machine (M2M) smart device reference architecture, TIA-4940.005. The document does not identify specific protocols to be used by the implementer, but rather, when taken in total, defines the requirements for communications pertaining to the access agnostic monitoring of bi-directional communication of events and information between logical entities, such as Point-of-Attachment and applications or networks.

Title of Standard	Description of Standard	Importance of Standard
TIA-942-A Telecommunications Infrastructure Standard for Data Centers	This document presents an infrastructure topology for accessing and connecting the respective elements in the various cabling system configurations currently found in the data center environment. In order to determine the performance requirements of a generic cabling system, various telecommunications services and applications were considered. In addition, this document addresses the floor layout related to achieving the proper balance between security, rack density, and manageability.	This Standard includes information for four tiers relating to various levels of availability and security of the data center facility infrastructure. Higher tiers correspond to higher availability and security. It is important to understand that certain intentional or accidental events, or acts of nature, pose a risk to the operation of data centers. It is important for the data center designer, administrator and manager to both assess and try to mitigate the risk to their facilities these events pose, as well as make contingency plans. The designer should provide a risk assessment, as well as ways to mitigate that risk. The standard also addresses considerations to improve the security of various portions of a data center facility, including the entrance room, main distribution area (MDA), intermediate distribution area (IDA), horizontal distribution area (HAD), zone distribution area (ZDA) and equipment distribution area (EDA).
TIA-568-C.1 Telecommunications Cabling Standard Addendum 1 – Pathways and Spaces	This Addendum specifies additional requirements, exceptions and allowances to ANSI/TIA-569-C for commercial buildings.	This standard provides standardized specific pathway and space design and construction in support of telecommunications media and equipment in commercial buildings. Requirements and considerations for the secure construction and layout of cable pathways and spaces in support of telecommunications media and equipment within multi-tenant buildings are provided.
ANSI/TIA-968-A Telecommunications – Telephone Terminal Equipment – Technical Requirements for Connection of Terminal Equipment to the Telephone Network	This document describes detailed cryptographic procedures for wireless system applications. These procedures are used to perform the security services of mutual authentication between mobile stations and base stations, subscriber message encryption, and key agreement within wireless equipment. This document contains both textual descriptions and reference implementations for the procedures. The textual descriptions are provided as an aid to the reader. In the event of a conflict between the text description and the reference code, it is recommended that implementations agree with the reference code.	This standard specifies technical criteria for terminal equipment approved in accordance with 47 CFR (Code of Federal Regulations) Part 68 for direct connection to the public switched telephone network, including private line services provided by wireline facilities owned by providers of wireline telecommunications. The technical criteria defined is intended to protect the telephone network from the harms defined in 47 CFR 68.3.

Title of Standard	Description of Standard	Importance of Standard
ANSI/TIA-569-C Commercial Building Standard for Telecommunications Pathways and Spaces	This standard specifies requirements for telecommunications pathways and spaces both within and between buildings.	This standard, and its related addendums, provide guidance for alternate routing of cabling into a building to help prevent loss of conventional and emergency communications and services.
TIA-946 Enhanced Cryptographic Algorithms	This standard, developed by the TIA TR-45 Ad Hoc Authentication Group, describes detailed cryptographic procedures for wireless system applications. The TR-45 Ad Hoc Authentication Group addresses cdma2000® packet data security requirements and is responsible for Security Assessment Issues, including IP-related aspects and selection of cryptographic algorithms that are supported within TR-45 Engineering Committee security mechanisms. The Group collaborates with the Third Generation Partnership Project (3GPP2) Technical Specification Group (TSG)-S, Working Group (WG) 4 (Security).	The procedures within TIA-946 are used to perform the security services of mutual authentication between mobile stations and base stations, subscriber message encryption and key agreement within wireless equipment.

8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

National. Consistent with our positions above, TIA believes that existing public-private partnerships should be utilized and augmented to facilitate greater information sharing, both from critical infrastructure operator to government and vice versa, rather than imposing new regulatory regimes that add on reporting requirements to existing ones. A complex myriad of national-level cybersecurity-related reporting requirements already exist, including:

Agency	Rule/Threshold
FCC	Wireline, wireless, cable, and satellite communications service providers, including interconnected Voice over Internet Protocol ("VoIP") service providers, must submit reports in the event that certain network outages reach the specified criteria and thresholds through the FCC's Network Outage Reporting System ("NORS").
FTC	Vendors of personal health records and related entities to notify consumers when the security of their individually identifiable health information has been breached.
FTC	Any financial institution that provides financial products or services to consumers must give consumers privacy notices that explain the institutions' information-sharing practices.
FTC	Requires companies to get parental approval before collecting online information from children under 13 years of age.

Agency	Rule/Threshold
FERC	Electric utilities operating bulk power system assets must comply with eight North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") standards.
HHS	Following a breach of unsecured protected health information, Health Insurance Portability and Accountability Act-covered entities must provide notification of the breach to affected individuals, the HHS Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred.
OMB/ DHS	Federal agency Chief Information Officers ("CIOs"), Inspectors General, and the Senior Officials for Privacy must submit to DHS' Federal Network Resilience division via CyberScope: (1) data feeds directly from security management tools; (2) government-wide benchmarking on security posture; and (3) agency-specific interviews.
SEC	Publicly traded United States companies must report information that is considered to have a substantial likelihood that a reasonable investor would consider it important in making an investment decision or if the information would significantly alter the total mix of information made available.[26]

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

Cybersecurity's scope and prospective bearing on national security and the overall United Staets and international economy has persistently grown. Like other aspects of the economy, critical infrastructure in the United States, such as the electric grid, water supply, transportation, financial systems and emergency services have all profited from increased assimilation of ICT to make structures more effective, resilient and reliable. Because of these benefits, it has become very advantageous to overlay critical infrastructure assets with industrial control systems and advanced communications systems. For example, the continual upgrading of the electric grid has had and will remain to have sweeping benefits including: empowering the incorporation of discontinuous energy from solar and wind sources into the grid, increased ease in electric vehicle proliferation, increased distributed generation possibilities, and decreasing line loss, among a host of other benefits.[27]

[26] *See* Basic Inc. v. Levinson, 485 U.S. 224 (1988); and TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438 (1976).

[27] TIA, *Smart Grid Policy Roadmap* (Feb. 2011) *available at* www.tiaonline.org/sites/default/files/pages/TIASmartGridPolicyRoadmap.pdf.

While it is widely accepted that critical infrastructure will continue to be subject to an increasing number of attacks,[28] TIA believes that both industry and policymakers widely recognize the necessity to protect ICT-enabled critical infrastructure and accompanying industrial control systems from cyber attacks. As networks shift towards IP, the overlay of organizational critical assets will continue to grow. We understand the pull that some policymakers may feel to silo their infrastructure as a result of increased cyber attack dangers. TIA believes that, enabled by successful efforts such as public-private partnerships, the use of voluntary and consensus-based standards, and other means to address threats noted above, this convergence can be a strength, and not a liability, to a secure and resilient infrastructure for each sector.

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

Discussed above in this submission are numerous efforts to ensure that organizations have the ability to provide essential services while managing cybersecurity risks. To what degree an organization's performance goals are used to ensure their ability to provide essential services while managing cybersecurity risk will be dependent upon the specific needs of their sector and organization. However, ICT manufacturers work with the gamut of organizations they supply to ensure that performance goals of that organization are reflected in the ICT they purchase. The flexibility to innovate and the use of voluntary, consensus-based standards are both key enablers of this capability.

11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

[28] For example, the Incident Response Summary Report from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported a 400% increase in reported and identified incidents impacting organizations that own and operate control systems associated with critical infrastructure from 2010 to 2011. ICS-CERT, *ICS-CERT Incident Response Summary Report 2009-2011*, 2 (Jun 2012) available at www.us-cert.gov/control_systems/pdf/ICS-CERT_Incident_Response_Summary_Report_09_11.pdf.

ICT manufacturers are currently affected by a number of regulations as noted above, namely those of the Federal Communications Commission adopted to ensure the resiliency and reliability of communications networks which service providers must comply with.[29] TIA members' products also comprise the provision of services across critical infrastructure uses, and our members work closely with their customer partners to ensure compliance with reporting obligations.

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

TIA believes that national/international standards and organizations that develop national/international standards should serve as a cornerstone in critical infrastructure cybersecurity conformity assessment. Standard developers and related organizations are already active in developing cybersecurity standards and conformity assessment, and should continue to play a key role. As we have described above in this response, several international standards cover cybersecurity conformity assessment across parts of the ICT landscape, such as SAFEcode, the Trusted Technology Forum, and the Common Criteria. Others are still being developed, such as the security assurance methodology for mobile networks now addressed by 3GPP Systems Aspects (SA) 3. These form part of the landscape of global standards and best practices that will continue to evolve in the future. Consequently the Framework should neither stifle innovation nor constrain such industry-driven evolution by any prescriptive regulation on conformity assessments.[30]

13. What additional approaches already exist?

---

[29] *See* 47 C.F.R. Part 4.

[30] Unfortunately, there are other parts of the globe where "foreign" input is disregarded, and the standardization system is effectively used as a way to give preference to parties physically located within a country. We believe that the United States government is in alignment with other standardization stakeholders that such policies stifle innovation and investment.

TIA believes that end-user education is also a crucial aspect to improving cyber threat ecosystem response capabilities, as many cyber vulnerabilities are already known and related attacks are relatively easily preventable. Numerous efforts exist across sectors to inform end users of proper steps to take to ensure that proper cyber "hygiene" is impressed. We support the CSRIC-based recommendation that network operators and service providers educate the customers on important steps that should be taken, from the use of adequate passwords to encryption of data.[31]

14. Which of these approaches apply across sectors?

Generally, standards and best practices are used heavily within the global ICT community as detailed above. As we also noted above, the ICT manufacturer community enables other sectors to successfully and securely communicate, and for this reason believe these trends to be present in most other if not all other individual sectors.

15. Which organizations use these approaches?

We believe that the vast majority, if not all, critical infrastructure owners and operators utilize public-private partnerships, standards, and best practices to address cyber risks. Across sectors, the owners and operators of critical infrastructure have the primary responsibility for the security of their networks and systems. We believe critical infrastructure owners and operators are motivated in addressing increasing and evolving cyber threats due to numerous factors, namely market pressures.

16. What, if any, are the limitations of using such approaches?

Significant investments in security from both operators and ICT vendors, strong network management, implementation of best practices and techniques, and voluntary coordination are all essential components of the current ecosystem that has protected critical infrastructure from

[31] *See* CSRIC Working Group 2A Report.

significant attacks. These components should continue to provide the foundation for critical infrastructure policy moving forward. In contrast, a mandatory regulatory regime for critical infrastructure would not serve the nation's cybersecurity needs well, and is much more difficult, generally, to alter and update as necessary in comparison. Consistent with our discussion above, we believe that while no system is perfect, the benefits of a system that uses voluntary coordination and heavily uses industry-developed consensus-based standards heavily outweigh those of a mandatory regulatory regime. This stated, we appreciate that the Framework will apply to owners and operators of critical infrastructure who voluntarily participate and other entities that may voluntarily participate.

17. What, if any, modifications could make these approaches more useful?

We caution NIST and policymakers generally that imposing rigid requirements in the Framework – requirements that by their nature will be unable to keep up with rapidly evolving technologies and threats – would require industry to focus on obsolete security requirements rather than facing the actual threat at hand, effectively making systems less secure. Instead, the key to improving the cybersecurity of critical infrastructure is to strengthen the broader cyber ecosystem that enables rapid information sharing, enhances public private partnerships, and provides sufficient investment to address current and emerging threats. We believe that the Framework should promote these benefits. Enabling ease in information sharing and maintaining the ability of owners and operators of critical infrastructure and their suppliers to innovate and make flexible decisions consistent with the above discussion should be a priority for the Framework that could help modify current approaches taken in this area.

18. How do these approaches take into account sector-specific needs?

As described above, each standard and best practice is not necessarily relevant for each area, sector, node, etc. of the communications industry. Because they are not mandated, network operators are allowed the flexibility to employ the best equipment and systems that meets their

specific challenges to cybersecurity and supply chain integrity. In this way the current approach allows for sector-specific needs to be accounted for.

19. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

NIST should keep in mind that there will be varying levels of preparedness and involvement across sectors, and that great care should be taken to avoid overgeneralized processes or standards across sectors. From the perspective of the communications industry, TIA does not believe that new standard development efforts or additional voluntary programs are need past existing efforts prior to the EO, and what NIST, DHS, and other agencies are effecting under the EO. Where a gap is identified in the process to develop the Framework, we believe that NIST should defer to voluntary and consensus-based processes already in existence in all instances possible.

20. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

Regarding public-private partnerships, we believe that these agencies are crucial partners in the successful public-private partnership efforts described above. In addition, the SCCs that include Federal agency interests should serve as hubs of information sharing – among members and between SCCs – to enable the use of effective approaches.

21. What other outreach efforts would be helpful?

TIA believes that it is critical that NIST and other USG representatives interact with and participate in the industry-led effort to develop voluntary, consensus-based standards, and encourages such engagement as soon as possible, as widely as possible. Aside from the benefits

of engagement in an ANSI-accredited standardization process such as TIA's,[32] engagement by the United States government (and NIST in particular) in the standards process will bolster the integrity of resulting standards, and effect increased adoption. This benefits all stakeholders involved in the standard development process, and TIA believes that NIST will find that realizing each of its goals for the Framework will be more easily attained through engagement in such a standards development process.

Specific Industry Practices

1. Are these practices widely used throughout critical infrastructure and industry?

The standards and best practices discussed above have been very widely adopted throughout the communications sector. For example, approximately 70% of standardized data center deployments utilize TIA's TIA-942.

2. How do these practices relate to existing international standards and practices?

The communications sector has been working on issues related to cybersecurity and supply chain integrity for longer than many other sectors. As a result, existing international standards and best practices are widespread amongst the ICT community; however if the circumstances warrant, decisions may be made to address unique supply chain and/or cybersecurity factors, illustrating the need for flexibility.

[32] Such benefits include, but are not limited to: consensus must be reached by representatives from materially affected and interested parties, standards are required to undergo public reviews when any member of the public may submit comments, comments from the consensus body and public review commenters must be responded to in good faith, and an appeals process is required. *See* ANSI, *ANSI Essential Requirements: Due process requirements for American National Standards* (Jan. 2010), *available at* http://publicaa.ansi.org/sites/apdl/Documents/Standards%20Activities/American%20National%20Standards/Procedures,%20Guides,%20and%20Forms/2010%20ANSI%20Essential%20Requirements%20and%20Related/2010%20ANSI%20Essential%20Requirements.pdf.

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

TIA members have found that several key efforts (described in more detail above), particularly the work in developing the Common Criteria and the work of the OTTF, should be considered some of the most critical efforts for secure operation of critical infrastructure.

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

Certainly, not all of the practices noted above will apply across sectors, but many in fact do. In evaluating specific sectors, we urge for NIST to seek consensus from those stakeholders as to what can be applicable to them. NIST's approach should be based on available best practices and standards that allow for a self-regulated model where parties with the most direct and relevant knowledge of the process can evaluate current practices and provide recommendations on how to minimize risk. The Framework's consistency with existing commercial best practices will encourage the broadest availability of products and services.

5. Which of these practices pose the most significant implementation challenge?

We believe that it is most appropriate for individual organizations to answer this question specific to their own practices.

6. How are standards or guidelines utilized by organizations in the implementation of these practices?

As noted above the standards and guidelines that have been developed by and for the ICT industry are used by organizations to address threats based on specific needs. We emphasize that a flexible and voluntary framework will allow for tailored and specific uses that reflect unique needs and threats.

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

ICT manufacturers and vendors generally have methodologies in place for the proper allocation of business resources to invest in, create, and maintain IT standards. As detailed above, the ICT standard development and best practice aggregation process is generally robust and global in nature.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

ICT manufacturers and vendors implement steps to formally escalate growing cybersecurity risks through the US-CERT and other information sharing mechanisms that exist through public-private partnerships. The fluidity of the standards process can also allow for some emerging cybersecurity and supply chain issues to be addressed in an efficient and prevalent way.

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

TIA is supportive of to refine approaches to cybersecurity that incorporate any legitimate concerns regarding privacy or civil liberties.

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

The NIST Framework will have a profound impact worldwide. It will impact every business with international presences and/or dealings – including many ICT manufacturers –along with policy decisions made by other countries. The cost implications for implementing the Framework, and the ensuing potential economic impact on the costs of delivering goods and services, remain

uncertain. Also uncertain are the degree to which adherence to the Framework will mesh with cybersecurity/critical infrastructure mandates that may be put in place in other countries.

For businesses, the approval and application of the Framework by owners and operators of critical infrastructure likely will extend to all aspects of a company's ecosystem, including outsourced service providers and companies within the supply chain. As we have described above, ICT products are frequently designed and manufactured in different places using globally-sourced components, making it problematic to categorize products as "U.S." or "non-U.S." products. Apart from the difficulty in determining whether a product is "U.S." or "non-U.S.," ICT companies undertake diverse aspects of their processes in multiple countries. We urge NIST to ensure that the Framework reflects that ICT companies need to continue to use a disseminated approach to their technology development and manufacturing. Any approach must involve international cooperation and substantial engagement with the private sector and should not include language that might put the government in a position to determine the future design and development of technology.

For governments, the U.S. must work with other governments to establish international security standards in order to prevent hamstringing industry with U.S.-only standards. TIA is concerned with the impact on global competiveness as well as technology innovation and development of having the U.S. government set specific technical standards. NIST should not enact cybersecurity policies that would restrict trade in telecommunications equipment imported to, or exported from, other countries that are part of the global trading system. Other countries cite similar concerns regarding foreign ICT equipment and are currently considering trade restrictive measures. TIA recommends that the U.S. government exercise extreme caution in how it approaches this issue since U.S. policy will effectively serve as a global standard. If the U.S. develops unique approaches that restrict trade unnecessarily, U.S. global economic competitiveness could be severely affected by other export markets adopting similar restrictive policies.

11. How should any risks to privacy and civil liberties be managed?

TIA is supportive of to refine approaches to cybersecurity that incorporate any legitimate concerns regarding privacy or civil liberties.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the framework?

TIA believes that end-user education is also a crucial aspect to improving cyber threat ecosystem response capabilities. We believe that the Framework should incorporate this aspect of cybersecurity and incorporate the CSRIC-based recommendation that network operators and service providers educate the customers on important steps that should be taken, from the use of adequate passwords to encryption of data.[33]

III. Conclusion

TIA congratulates NIST on its work and progress on the Framework, and the opportunity for comment in this matter. We urge the consideration of the above views on the part of the ICT manufacturer, supplier, and vendor community, and we look forward to future engagement with NIST and other Federal agencies as information system policies are formulated and implemented pursuant to the Executive Order.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: */s/ Danielle Coffey*

Danielle Coffey
Vice President & General Counsel, Government Affairs

Dileep Srihari

[33] *See* CSRIC Working Group 2A Report.

Director, Legislative & Government Affairs

Brian Scarpelli
Senior Manager, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 Court House Road
Suite 200
Arlington, VA 22201
(703) 907-7700

April 8, 2013