TIA
ADVANCING GLOBAL COMMUNICATIONS

TELECOMMUNICATIONS
INDUSTRY ASSOCIATION

1320 N. Courthouse Rd., Suite 200
Arlington, VA 22201 USA
www.tiaonline.org

Tel: +1.703.907.7700
Fax: +1.703.907.7727

April 29, 2013

Via Electronic Filing

Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

Re: Comments of the Telecommunications Industry Association to the National Institute of Standards and Technology and National Telecommunications and Information Administration on *Incentives To Adopt Improved Cybersecurity Practices* (Docket Number 130206115–3115–01)

I. Introduction and Statement of Interest

The Telecommunications Industry Association ("TIA") hereby submits comment on the National Institute of Standards & Technology's ("NIST") and National Telecommunications and Information Administration's ("NTIA") Notice of Inquiry ("NOI") requesting information to inform its effort to develop recommendations on incentives to adopt improved cybersecurity practices.[1] The Executive Order ("EO") directs the Department of Commerce to recommend ways to promote participation in the Department of Homeland Security's ("DHS") Critical Infrastructure Cybersecurity Program ("Program"), and states that the recommendations "shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants of the Program." The Department of Commerce must then submit its recommendations to the President through the Assistant to the President for Homeland Security

[1] National Institute of Standards and Technology; National Telecommunications and Information Administration, *Incentives To Adopt Improved Cybersecurity Practices*, Notice of Inquiry, 78 Fed. Reg. 18954 (Mar. 28, 2013) ("NOI"); Executive Order – Improving Critical Infrastructure Cybersecurity, rel. Feb. 12, 2013 ("EO").

and Counterterrorism and the Assistant to the President for Economic Affairs no later than June 12, 2013.

We appreciate the Administration's efforts to augment voluntary participation in enhanced cybersecurity practices. Below, in our responses to the questions posed by NIST and NTIA in the NOI, we urge that these agencies proceed in its development of recommendations on incentives to the President, per 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 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")

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

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

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.[5]

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

[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).

[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.

formulation of United States positions on technical and policy issues, administering four International Secretariats and 16 U.S. Technical Advisory Groups 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 machine-to-machine ("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]

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

II. TIA Responses to Questions Posed in the NIST/NTIA Notice of Inquiry

1. Are existing incentives adequate to address the current risk environment for your sector/company?

Currently, the ICT industry has a number of incentives to address security issues in concert with their customers across sectors. However, as discussed elsewhere in this response, key incentives are lacking. *Existing* incentives include the following:

Leveraging public-private partnerships. TIA believes that existing incentives to improve cybersecurity include existing public-private partnerships. These are an effective tool for collaboration on addressing current and emerging threats, and will serve as a key incentive to encourage businesses to make investments in cybersecurity that are appropriate for the risks that they face. 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,[10] 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

[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.

[10] For example, it was recently reported that state-sponsored cyberespionage incidents (just one category of a type of cyber attack) have tripled over the last year. *See* Verizon, 2013 Data Breach Investigations Report (rel. Apr. 2013), *available at* http://www.verizonenterprise.com/DBIR/2013/.

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 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.[11]

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 Communications, Security, Reliability and Interoperability Council ("CSRIC"), and the National Security Telecommunications Advisory Committee ("NSTAC"). These and other public-private partnerships have demonstrated themselves as effective means in giving industry required flexibility to prevent attacks, and should serve as the foundation for moving forward

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

with critical infrastructure protection. Their success serves as a model – and an incentive for others to join.

TIA notes its strong belief 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.

The recognized need for standards and best practices. We believe that the US Government already understands that network reliability is affected by a broad array of factors that may help or hurt the network, including software, hardware, human, and inter-government relationship factors.[12] For example, the National Security Telecommunications Advisory Committee ("NSTAC") acknowledged the diverse factors involved with improving networks when it stated that "the evolution of the communications network will be driven by changes in technology, applications, content, devices, and increased requirements for capacity, bandwidth, and spectrum."[13] Discussed in TIA's related filing to NIST to inform the development of its Cybersecurity Framework are numerous efforts to ensure that organizations have the ability to provide essential services while managing cybersecurity risks.[14] Many of these standards and best practices are used in industry segments across critical infrastructure categories, incentiving existing as well as new entrants into these segments to adopt the practices as well as participate in their development.

Competitive differentiation and business continuity. ICT manufacturers and vendors work to meet the needs of their customers. Naturally, less secure products that are more vulnerable to cyber attacks will be less attractive to both critical infrastructure owners and operators, as well as

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

[13] NSTAC, *NSTAC Report to the President on Communications Resiliency* (rel. Apr. 19, 2011) at 4 (NSTAC 2011 Report).

[14] *See* TIA Cybersecurity Framework Comments at 14-16.

end-users, and this drives ICT manufacturers and vendors to strive to make their products and services less susceptible to cyber attacks. To illustrate how much this concept drives enhanced cyber defenses in ICT products and services, we note that it is estimated that Global Cyber Security spending is expected to reach $60 billion in 2011 and is forecast to grow at 10 percent every year during the next three to five years.[15] As we described in our submission to NIST on the planned Cybersecurity Framework, [16] 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 range of organizations they supply to ensure that performance goals of those organizations 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.
Certainly, the concept of improving product and service security based on competitive differentiation needs is not specific to the communications sector. We urge NIST and NTIA to keep this in mind when making recommendations on incentives to adopt improved cybersecurity practices, and to take great care to avoid altering this virtuous effect.

2. Do particular business sectors or company types lack sufficient incentives to make cybersecurity investments more than others? If so, why?

Generally, when comparing incentives to invest in cybersecurity amongst business sectors, differences can be attributed to two major factors: (1) the degree to which the product or service is "critical;" (2) how competitive the industry segment is. As we also discuss below, cybersecurity-themed regulatory mandates – which exist in some business sectors while not in others – do not directly correlate to associated investment in cybersecurity technologies.

[15] *See* PwC, *Cyber Security M&A: Decoding deals in the global Cyber Security industry* (Nov. 2011), *available at* http://www.pwc.com/gx/en/aerospace-defence/publications/cyber-security-mergers-and-acquisitions.jhtml.

[16] *See* Comments of TIA, *Developing a Framework To Improve Critical Infrastructure Cybersecurity* (Docket Number 130208119–3119–01), filed Apr. 8, 2013, *available at* http://www.tiaonline.org/sites/default/files/pages/TIA_Comments_NIST_Cybersecurity_Framework_040813.pdf ("TIA Cybersecurity Framework Comments").

The critical nature (i.e. the degree that a cyber attack could potentially cause harm) of a product or service will determine, to a significant degree, the level of cybersecurity investment. In this sense, sectors such as electricity and telecommunications have a heightened incentive to invest in cybersecurity than some other sectors. In other words, the more widespread harm that a cyber attack can incur, the more incentive there is to invest to prevent such attacks. But it is important to note that sector vulnerability to cyber attack is also a function of the concentration of critical assets under one or a few points of control. Regulatory incentives that reward concentration of assets – "putting all the eggs in one basket" – will heighten the vulnerability to cyber attacks and may result in less cybersecurity protection.[17]

Second, a notable factor that drives cybersecurity investment incentives among business sectors is the degree to which that sector is competitive. Coupled with the critical nature of a business sector, increased competition will drive heightened cybersecurity investment mainly due to market differentiation needs discussed above. For example, the banking and telecommunications business sectors, which are highly competitive and have many market entrants, will have an increased incentive to make cybersecurity investments over other business sectors, such as the water or railroad business sectors, which have relatively less market entrants. In short, competition drives investment and innovation. Competition also enables wide distribution of points of control under many entities and a diversity of approaches to defend against cyber attack, lowering the potential for widespread harm from cyber attack.

The imposition of cybersecurity regulations alone will not be effective in incenting investments. As we have long held, regulatory mandates that require the use of specific technology for business sector security will not allow technology to evolve in response to rapidly changing threat conditions or effectively incent investments in new technologies that can provide heightened cyber attack resiliency. An open a collaborative approach is a more productive approach. One example of government actions that have taken this approach is the National

[17] *See*: Comments of FERC Chairman Jon Wellinghoff ("A more distributed system is much more resilient," he said. "Millions of distributed generators can't be taken down at once.") at: http://www.bloomberg.com/news/2013-04-23/rooftop-solar-seen-protecting-u-s-power-grid-from-attack.html.

Cybersecurity Center of Excellence (NCCoE), a partnership between NIST, the State of Maryland and Montgomery County, that is dedicated to furthering innovation through the rapid identification, integration and adoption of practical cybersecurity solutions.[18] NCCoE integrates commercially available technologies to build practical cybersecurity solutions that can be rapidly applied to the real challenges that businesses face each day. The NCCoE has a straightforward, four-step process: (1) define the problem statement and frame it as a project; (2) assemble a team of members of industry, government and academia; (3) build practical solutions—based on commercially available technology—that are usable, repeatable and secure; and (4) facilitate rapid, widespread deployment and use of these solutions. TIA commends this open and cooperative approach that NIST is following.

3. How do businesses/your business assess the costs and benefits of enhancing their cybersecurity?

It is ICT manufacturers, integrators and value-added resellers who enable each critical infrastructure sector to function and to communicate securely. In that context, defining and assessing the costs and benefits of enhancing cybersecurity resiliency is a unique evaluation that considers numerous factors that may help or hurt the network, including software, hardware, human, and inter-government relationship factors.[19] Other important factors include those noted in the 20 Critical Controls,[20] all of which were recently determined by the FCC's CSRIC to be applicable to the enterprise communications networks.[21]

[18] *See* NIST Federal Register notice "Proposed Establishment of a Federally Funded Research and Development Center-First Notice" (April 22, 2013) at: https://federalregister.gov/a/2013-09376

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

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

[21] *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.

4. **What are the best ways to encourage businesses to make investments in cybersecurity that are appropriate for the risks that they face?**

Past the *existing* incentives noted above in response to Question 1, we submit the following suggestions on ways to encourage businesses to make investments in cybersecurity that are appropriate for the risks that they face:

Maintain the flexibility and the ability to innovate. When forming recommendations towards incentivizing businesses to make investments in cybersecurity that are appropriate for the risks that they face, the danger inherently exists to overgeneralize. TIA believes that an utmost concern for NIST and NTIA in forming their recommendations to the President must be to respect the need for specific sectors to innovate and to address specific threats.

"Critical infrastructure," was identified by DHS pursuant to Presidential Policy Directive #7 in 2003.[22] Under the EO, not later than July 12, 2013, the Secretary of Homeland Security must 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 commercial information technology products or consumer information technology services" under this process. TIA again notes our support for 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 critical infrastructure sector 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

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

cybersecurity across sectors. TIA urges the Department of Commerce, in forming its recommendations to the President and in other efforts to implement the EO, reflect this important need.

Enhanced information sharing. Lacking the capability to efficiently share crucial and timely cybersecurity data and information while ensuring strong liability and privacy protections is a significant barrier to making investments in enhancing cybersecurity capabilities across critical infrastructure business sectors. TIA encourages all government actors to eliminate major obstacles to information sharing and to facilitate cooperation in defense against cyber attacks, and that added certainty will incent businesses to make investments in cybersecurity that are appropriate for the risks that they face. 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.[23] Liability protection for organizations that disclose information in good faith as part of an information sharing program will serve as a crucial incentive to invest in cybersecurity.

Increase Federal 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.[24] 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."[25] TIA maintains that the United States government has not offered or

[23] 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.

[24] 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.

[25] 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.

effected the commitment needed to avert this risk: Federal investment in ICT research remains comparatively low when compared to other scientific fields. Federal funding for cybersecurity research and development should be prioritized, and should coordinate research activities amongst contributing agencies, incorporating industry input. Placing a priority on Federal research and development in the cybersecurity field will demonstrate that the Federal government understands this need and will incentivize industry to do the same. NIST has announced its intention to sponsor a Federally Funded Research and Development Center (FFRDC) to help the NCCoE address industry's needs most efficiently. When established, this will be the first FFRDC founded by the Department of Commerce and the only one in the nation devoted to cybersecurity.[26] TIA commends this investment.

Providing tax-based incentives. We agree with previous comments submitted to the Internet Policy Task Force ("IPTF") on incentives to adopt cybersecurity best practices that the Federal government could quite effectively increase incentives to invest in cybersecurity by providing tax credits for such investments.[27] While further consultation would be needed from a variety of stakeholders, we support the Department of Commerce recommending tax-based incentives to the President.

Cybersecurity insurance. As the Internet Policy Task Force noted in 2011, cyberinsurance can (1) promoting widespread adoption of preventative measures throughout the market; (2) encourage the adoption of best practices; and (3) limit the level of losses businesses may face following a cyber attack.[28] TIA agrees that cyberinsurance can serve as an incentive to companies to take proactive steps to improve cyber attack resilience.

[26] See NIST Press release (April 22, 2013) at: http://www.nist.gov/itl/nccoe-042213.cfm

[27] Dept. of Commerce, *Cybersecurity, Innovation, and the Internet Economy* (June 2011), http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf ("IPTF Green Paper").

[28] IPTF Green Paper at 24. http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf

Recognizing the necessity of international approaches and standards. TIA urges NIST and NTIA to ensure that their recommendations to the President reflect 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 the recognition 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. Moreover, to control costs and manage supply chain risk, manufacturers need flexibility to change component suppliers for a particular product at any time. 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 and NTIA'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 by the Federal government 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.

5. **How do businesses measure success and the cost-effectiveness of their current cybersecurity programs?**

It is ICT manufacturers , integrators, and value-added resellers who enable each critical infrastructure sector to function and to communicate securely. In that context, defining and assessing the cost effectiveness of a business' cybersecurity program is a unique evaluation that considers numerous factors.[29] Past this statement, we believe that it is most appropriate for individual organizations to answer this question specific to their own practices.

6. **Are there public policies or private sector initiatives in the United States or other countries that have successfully increased incentives to make security investments or other investments that can be applied to security?**

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; each successfully increases incentives to make security investments or other investments that can be applied to security. These efforts occur domestically and internationally. TIA has aggregated an

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

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/).
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).

Name of SDO/Consortia/Fora	Description
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).
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 the Department of Commerce's consideration in its consideration under the NOI.

TIA has undertaken an effort to determine its standards activities that support cybersecurity and supply chain integrity, and increase incentives to make security investments or other investments that can be applied to security. The various TIA committees[30] considered include TR-42 Telecommunications Cabling Systems, TR-45 Mobile and Personal Communications Systems

[30] 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.

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 efforts, with explanations of applicability, can be viewed below:

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.

Title of Standard	Description of Standard	Importance of Standard
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.
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.

Title of Standard	Description of Standard	Importance of Standard
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.
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.

7. **Are there disincentives or barriers that inhibit cybersecurity investments by firms? Are there specific investment challenges encountered by small businesses and/or multinational companies, respectively? If so, what are the disincentives, barriers or challenges and what should be done to eliminate them?**

There are numerous disincentives and barriers that inhibit cybersecurity investments by firms, including but not limited to:

- **Regulatory requirements that discourage market-driven investment:** As we discuss above, cybersecurity-themed regulatory requirements currently exist for some business sectors. These mandates do not leverage collaboration and cooperation as effectively as public-private partnerships, instead offering compliance in lieu of penalty; do not allow for instance-specific and tailored decisions to be made by those organizations closest to cyber attacks; and may result in duplicative and expensive requirements that do not permit assets to be concentrated on protection rather than outmoded mandates. This effect – particularly the latter – can be seen at a Federal agency that does have cybersecurity mandates for the industry it regulates: the Federal Energy Regulatory Commission ("FERC") has very recently proposed to approve proposal to transition from the currently-effective CIP version 3 Standards to compliance with the CIP version 5 Standards, skipping version 4 due to its outdatedness and delays in implementation of the mandate.[31]
- **Liability:** When there is a risk of serious liability, there is also an inherent disincentive to take risk and enter a market. As we have described above, the assurance of liability protection for organizations that disclose information in good faith as part of a two-way information sharing program will serve as a crucial enabler of this incentive (for both industry and government).
- **Firm-specific economics:** Depending on economic conditions and the state of a firm, investment in cybersecurity may vary.
- **Market concentration:** Industries which are dominated by only a few entities are less likely to support robust innovation due to the lack of a competitive incentive to invest in the development of cybersecurity technologies.

[31] FERC NOPR (April 18, 2013).

8. Are incentives different for small businesses? If so, how?

TIA, with a membership comprised of ICT businesses of all sizes, understands and appreciates that small businesses are a crucial driver of the American economy. Small businesses and startups may not have the resources to invest in the prevention of cyber attacks to the degree that large corporations do, while at the same time are at a greater risk of failing and may also hold very innovative intellectual property. While the stakes may be higher for some smaller businesses for the above reasons, larger businesses experience the same circumstances to varying degrees, and the cause and vector of a cyber attack will not necessarily be different based on the size of a business (i.e. general cybersecurity "hygiene" is a major cause of attacks for businesses of any size). These considerations are important in the Department of Commerce's formulation of recommendations to the President.

9. For American businesses that are already subject to cybersecurity requirements, what is the cost of compliance and is it burdensome relative to other costs of doing business?

ICT manufacturers and vendors provide innovative products and services that the make up the systems which enable the functioning of all critical infrastructure. As we have discussed in our submission to NIST on the Cybersecurity Framework, various firms and Federal agencies themselves are subject to cybersecurity regulations on the Federal level, including the following agencies: the FCC, the Federal Trade Commission ("FTC"), FERC, the Department of Health and Human Services ("HHS"), the Office of Management ("OMB"), DHS, and the Securities and Exchange Commission ("SEC").[32] Compliance with these regulations can easily overlap, and may also easily require the hiring of dedicated staff, usually legal. In short, compliance with cybersecurity-related reporting regulations is expensive, and ICT manufacturers and vendors work diligently with our customers to ensure that their reliability and resiliency needs are met.

[32] TIA Cybersecurity Framework Comments at 19-20.

Past the above response, we believe that it is most appropriate for individual organizations to answer this question specific to their own practices.

10. **What are the merits of providing legal safe-harbors to individuals and commercial entities that participate in the DHS Program? By contrast, what would be the merits or implications of incentives that hold entities accountable for failure to exercise reasonable care that results in a loss due to inadequate security measures?**

Standards may be used to define an acceptable level of performance, and through participation in the process, a governmental entity can work to ensure that an adequate level of service is offered to the public in a particular area. In some limited instances, the government has made standards legally binding to assure a minimum level of public safety through safe harbors.[33] In addition, standards may also be used by government entities as valuable sources of scientific and technical information, allowing for agencies to use standards as a resource for advanced technical information without first-hand independent knowledge of research in the area. TIA supports the use of industry-led, voluntary, consensus-based standards as safe harbors, but not as requirements; such a legal structure allows for technology-neutral regulation while ensuring a reasonable certainty of liability protection. Another way to reduce liability risk for development of cybersecurity tools would be to extend the protection of the SAFETY Act (Support Anti-terrorism by Fostering Effective Technologies) to cover cybersecurity tools. The SAFETY Act preempts and modifies tort law for “qualified” anti-terrorism technologies, and limits tort liability to verified amount of available insurance. The goal of the SAFETY Act is to encourage

[33] Section 107(a)(2) of CALEA contains a safe harbor provision, stating that "[a] telecommunications carrier shall be found to be in compliance with the assistance capability requirements under section 103, and a manufacturer of telecommunications transmission or switching equipment or a provider of telecommunications support services shall be found to be in compliance with section 106 if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the Commission under subsection (b), to meet the requirements of section 103." 47 U.S.C. § 1006(a)(2). Subcommittee TR-45.2 of TIA, along with Committee T1 of the Alliance for Telecommunications Industry Solutions, developed interim standard J-STD-025 to serve as a "safe harbor" for wireline, cellular, and broadband PCS carriers and manufacturers under section 107(a) of CALEA. The standard defines services and features required by wireline, cellular, and broadband PCS carriers to support lawfully authorized electronic surveillance, and specifies interfaces necessary to deliver intercepted communications and call-identifying information to a law enforcement agency. *See* TIA, Communications Assistance for Law Enforcement Act (CALEA), *available at* http://www.tiaonline.org/standards/technology/calea/ (last visited February 22, 2011).

the development and deployment of new and innovative anti-terrorism products and services by providing liability protections.[34]

11. What would be the impact of requiring entities to join the DHS Program prior to receiving government financial guarantees or assistance in relevant sectors?

We first note that this question is extremely difficult to answer because the Framework has not yet been completed. In fact, the public is not even yet aware of what the structure of the document will look like, much less what its contents will be.

However, we believe that, without question, the most important aspect of the Framework is its voluntary nature. The EO goes to lengths to emphasize this. We emphasize again that, consistent with the above, that mandatory requirements, or policies that effectively act as mandates, will not leverage collaboration and cooperation as effectively as public-private partnerships; will not allow for instance-specific and tailored decisions to be made by those organizations closest to cyber attacks; and could result in duplicative and expensive requirements that do not permit assets to be concentrated on protection. While the EO requires a re-examination of Federal procurement *requirements* on those who choose to engage the Federal government, that is a separate endeavor from the DHS Program and the Cybersecurity Framework, and we believe that requiring businesses to join the DHS Program prior to receiving, for example, a cybersecurity tax credit or cybersecurity research and development grant, could effectively make the Framework's "recommendations" mandatory. We urge the Federal government to very carefully consider actions such as these in the implementation of the EO.

12. How can liability structures and insurance, respectively, be used as incentives?

As we have detailed above in responses above, liability protection for good faith actions is a needed component of any two-way cybersecurity information sharing program between

[34] For further details see the Department of Homeland Security SAFETY Act website at: https://www.safetyact.gov/pages/homepages/Home.do.

government and the private sector. Adequate liability protection will remove a large disincentive for critical infrastructure owners and operators to share important and timely information with the Federal government (and vice versa).

In addition, consistent with our comments above, we agree that cybersecurity insurance can help decrease cyber attacks by encouraging general implementation of preemptive processes; encourage the adoption of best practices, and; and may limit the losses a critical infrastructure owner or operator may face following a cyber attack.

13. **Should efforts be taken to better promote and/or support the adoption of the Framework or specific standards, practices, and guidelines beyond the DHS Program? If so, what efforts would be effective?**

This question is extremely difficult to answer because the Framework has not yet been completed. In fact, the public is not even yet aware of what the structure of the document will look like, much less what its contents will be. This said, TIA does not believe that any further efforts should be undertaken to promote the adoption of the Framework past what the EO requires Federal agencies to do.

14. **In what way should these standards, practices, and guidelines be promoted to small businesses and multinationals, respectively, and through what mechanisms? How can they be promoted and adapted for multinational companies in various jurisdictions?**

As we have noted above, the Framework should reflect the priority for U.S.-based technologies' continued success in the global marketplace has been enabled through the development of internationally-used standards and best practices, and 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. In short, the best way to incentivize the adoption of the Framework by small businesses or multinationals (or any business) is to ensure that the Framework does not create a U.S.-specific approach that ignores industry-driven best practices and global standards.

15. What incentives are there to ensure that best practices and standards, once adopted, are updated in the light of changing threats and new business models?

As we have described above, standard and best practices that are driven by an industry-led, voluntary, and consensus-based process will best respond to changes in markets, technologies, etc. It is these aspects of standards and best practices – fluidity and responsiveness – that make them so much more effective than a mandate. With this said, if the Framework successfully incorporates existing standards and best practices efforts and can exist as a "living document," existing incentives – appropriately adopting changes based on the open and inclusive standards process – will ensure that the same are updated in the light of changing threats and new business models.

III. Conclusion

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, NTIA, and other Federal agencies as 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
Director, Legislative & Government Affairs

Brian Scarpelli
Senior Manager, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
10 G Street N.E.
Suite 550
Washington, D.C. 20002
(202) 346-3240

April 29, 2013