September 9, 2016

Nakia Grayson
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Via e-mail to: cybercommission@nist.gov

RE: ITI /ITAPS Input to the Commission on Enhancing National Cybersecurity RFI - "Information on Current and Future States of Cybersecurity in the Digital Economy"

Dear Ms. Grayson:

The Information Technology Industry Council (ITI) and the IT Alliance for Public Sector (ITAPS) appreciate the opportunity to respond to the Commission on Enhancing National Cybersecurity's (Commission) Request for Information (RFI), "Information on Current and Future States of Cybersecurity in the Digital Economy," as noticed by the National Institute of Standards and Technology (NIST) on August 10, 2016.

ITI is the global voice of the tech sector. We are the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry, and this year we are pleased to be commemorating our centennial. ITI's members comprise leading technology and innovation companies from all corners of the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, Internet companies, and companies using technology to fundamentally evolve their businesses. ITAPS, a division of ITI, is an alliance of leading technology companies building and integrating the latest innovative technologies for the public sector market. With a focus on the federal, state, and local levels of government, as well as on educational institutions, ITAPS advocates for improved procurement policies and practices, while identifying business development opportunities and sharing market intelligence with our industry participants. Cybersecurity is critical to both ITI and ITAPS members' success—the protection of our customers (including governments, businesses, and consumers), the privacy of individuals' data, our brands, and our intellectual property are essential components of our businesses, and impact our ability to grow and innovate in the future. Consequently, ITI and ITAPS have been leading voices in advocating effective approaches to cybersecurity - globally, domestically and at the state and local level - and across the commercial and federal procurement sectors.

Cybersecurity is rightly a priority for governments around the world, including the United States government (USG). Our members are global companies, doing business in countries around the world, and we share a common goal with all governments of improving cybersecurity. Most of our companies service the global market via complex supply chains in which products are developed, made, and assembled in multiple countries, servicing customers that typically span the full range of global industry sectors, including banking, telecommunications, energy and healthcare, as well as government customers. As a result, we acutely understand the impact of governments' policies on security innovation and the need for U.S. policies to be compatible with – and drive – global norms, as well as the potential impacts on our customers. As both producers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy. In the technology industry and other global industry sectors, when discussing any cybersecurity policy, it is important to consider our connectedness, which is truly global and borderless.

A central element of ITI's global advocacy efforts involves helping governments understand the critical importance of cross-border data flows, not only to the ICT sector, but also to the global economy as a whole. Virtually every business that operates internationally relies instinctively on the free and near instantaneous movement of data across borders to enable their day-to-day business operations, from conducting research and development, to designing and manufacturing goods, to marketing and distributing products and services to their customers, to securing global networks and the personal data of customers across the globe. In particular, U.S. and global ICT companies have a long history of exchanging security-related information across borders with geographically-dispersed employees, users, customers, governments, and other stakeholders, which helps them protect their own systems and maintain high levels of security for the technology ecosystem as a whole. We urge the Commission to make certain its forward-looking recommendations are reflective of the critical importance of global data flows to continued economic development, Internet growth, and of course, cybersecurity.

ITI and ITAPS submit our comments against the foregoing backdrop. We have not endeavored to comment on all of the topic area challenges and potential approaches identified by the Commission in the RFI, but instead focus our comments on the key issues that we believe will prove most helpful to the Commission in framing this complex and important subject for the next Administration and beyond. We organize our discussion of these issues under the overarching topic headings identified by the Commission, as appropriate. In addition, immediately below we offer our summary recommendations.

Summary Recommendations

Further the Framework Approach Domestically and Globally. The visionary work led by NIST, in cooperation with the private sector and other stakeholders, to develop the voluntary Framework for Improving Critical Infrastructure Cybersecurity[1] (the "Framework") should not be abandoned by the next or future U.S. Administrations. The Framework leverages public-private partnerships, is grounded in sound risk management principles, and helps foster innovation due to its flexibility and basis in global standards. The Framework has also consistently been lauded for providing a common language to better help organizations comprehend, communicate and manage cybersecurity risks. While it is important to stress that we are still in the early phase of a multi-year effort, we believe the Framework has already helped and will continue to help improve cybersecurity, and we believe the Framework approach worth prioritizing and replicating domestically and globally for organizations of all types.

[1] *See* NIST Framework for Improving Critical Infrastructure Cybersecurity, http://www.nist.gov/cyberframework/index.cfm

Streamline Federal, State and Local Cybersecurity Regulatory Efforts. Promoting the use of the Framework as a policymaking tool deserves greater focus. While the Framework has frequently been cited as providing a common language which can help companies better communicate risk management to improve cybersecurity internally (for instance with company executives or boards) and externally across their ecosystems (such as with business partners including suppliers), the potential of the Framework to provide a common language or taxonomy for policymakers globally, and at all levels of government, has not yet been fully realized. In particular, promoting the Framework as a common language for policymakers can help align US federal agency cybersecurity and risk management efforts by orienting them toward the Framework. We urge the Commission to recommend that federal agencies use the NIST Cybersecurity Framework government-wide to help agencies determine cyber risk, and explore how the Framework could be applied in the procurement.

Continue to Prioritize and Resource International Cybersecurity Standardization. Complementing the current Administration's ongoing support for the Framework, the USG earlier this year kicked off another policy initiative aimed at furthering international standards, launched via the *Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity* (the "International Standardization Strategy"). We recommend that future administrations prioritize furthering this strategy to improve the U.S. government's participation in the development and use of international standards for cybersecurity.

Assess and Leverage Existing Initiatives and Build upon existing Public-Private Partnerships. There has been a flurry of cybersecurity policymaking activity in the U.S. over the past few years (including multiple Administration executive actions dealing with cybersecurity, including EO 13718 that launched the Commission, and prominent cybersecurity laws passed by Congress (including CISA). These new initiatives complement well-established public-private partnership activities, and together the public and private sector have just begun implementing and utilizing many of these policy instruments. The Commission should assess this existing collaborative work before making new recommendations to future Administrations, in order to provide policymakers with a clear roadmap for holistic strategy execution.

Nurture IoT Development by Avoiding Siloed Regulatory Approaches. It is counterproductive to create siloed approaches to cybersecurity across variegated IT applications simply because more and more "things" become connected to the Internet in an increasingly digitized world. Indeed, to fully realize the benefits offered by the Internet of Things (IoT) and innovations such as Big Data Analytics, the USG should promote policies that help break down barriers to connecting devices and correlating data. Efforts to improve IoT cybersecurity, too, should leverage public private partnerships and build upon existing initiatives and resource commitments.

Adopt Policies that Facilitate Cross-Broder Data Flows Necessary for Cyber Defense. The Commission should ensure that policy measures the USG takes to enhance cybersecurity reflect the global nature of cyberspace. In particular, the USG and all governments should allow and facilitate cross-border data flows as the foundation of innovation and efficient development. To expedite broader adoption and benefit of these technologies, the USG should advocate globally against countries imposing measures requiring the local storage or processing of data or the use of local facilities, hardware, or services.

Prioritize Investment in Cybersecurity Workforce Development and Training. Prioritize paying down the "cyber debt" and reversing the current cybersecurity talent shortage. In particular, we recommend expanding initiatives like the CyberCorps Reserve program and standing up a Cyber National Guard to train and recruit new talent and protect public and private digital infrastructure.

Harmonize Federal Cybersecurity Acquisition Efforts and Apply Them Consistently Across the Federal Enterprise. As the Commission is doubtless aware, security is essential to the federal government mission and should no longer be treated and addressed in a patchwork, uncoordinated fashion. Allowing the furtherance of uncoordinated security approaches will simply continue the current model and perpetuate a security regime that is only as strong as the weakest link. We recommend that OMB harmonize all federal cybersecurity acquisition efforts to ensure that they are applied consistently across the entire federal enterprise, in order to develop an efficient and effective cybersecurity acquisition infrastructure. Without such oversight, an array of new requirements, regulation and guidance will add further confusion for the acquisition community, increase the compliance burden for both the government customer and the vendor community. Further, from a procurement standpoint, the Federal Government should continue to leverage existing technologies and capabilities that have proven successful in helping to secure agency information systems before investing to develop new capabilities that are duplicative of existing capabilities and thus fail to provide incremental value.

Allocate Federal Resources to Fund State and Local Government Investments in Cybersecurity. It is important that state and local governments prioritize information security and utilize existing federal cybersecurity grant programs. The federal government must continue to allocate resources and expertise to state and local governments to ensure that the vast amount of personally identifiable information (PII) held by state governments is adequately protected and prioritized, for instance, by empowering DHS to create a cyber security grants program to fund state and local government investments in cybersecurity.

Critical Infrastructure Cybersecurity: Advancing and Expanding the Framework Approach

ITI and ITAPS commend NIST's continuing work, in cooperation with the private sector and other stakeholders, to further the development of the Framework. The Framework leverages public-private partnerships, is grounded in sound risk management principles, and helps foster innovation due to its flexibility and basis in global standards. We believe the Framework has already helped and will continue to help improve cybersecurity, and we remain committed to helping it succeed.

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

Our own baselines of understanding notwithstanding, we believe the Framework has had and continues to have an important, valuable impact on organizations' understanding of cyber risks. The Framework has allowed organizations to have useful conversations about cybersecurity risk management both internally (e.g. with our senior management) and externally (e.g. with boards of directors, partners, suppliers, and customers), allowing these parties to better understand the importance of managing cyber risks. The Framework's common terminology (identify, prevent, detect, respond, recover) provides a flexible, common, standardized language to enable these discussions. To further expand the Framework's impact to better protect critical infrastructure as well as all organizations, we recommend the following:

Leverage Mapping to International Standards. The Framework's mapping to international standards such as ISO/IEC 27001 is helpful, as such standards help organizations establish an immediate linkage between their ongoing risk management and certification efforts. This type of mapping provides an extremely persuasive example to share with governments outside of the United States that may be considering their own national cybersecurity frameworks/initiatives. By mapping the Framework's security guidance to global standards, the Framework demonstrates that national cybersecurity concerns can be addressed in a manner that bolsters global standards.

Expand use of the Framework by suppliers. In recognition of the importance of addressing global supply chain security concerns, some companies have begun exploring how to expand Framework use with their suppliers. Two types of instances in which owners and operators of critical infrastructure (CI) services should consider requiring use of the Framework across their supply chains are: (1) where an owner/operator has outsourced the management of any part of its operation via a managed services partnership; and (2) where the supplier is considered a critical business partner, such that any disruption of their business would affect the delivery of critical services. Companies can also take proactive steps to encourage use of the Framework across by their ecosystem partners by, for example, integrating the Framework into their supplier guidelines.

Develop implementation guidance for SMBs. Not all companies have mature programs or the technical expertise to keep up with the latest developments in cybersecurity – such as the Framework – to appropriately manage cyber risk. SMBs in particular have reported being confused and even overwhelmed by the size and complexity of the current Framework. Given the interconnected nature of the cyber ecosystem, we are keenly aware that cyber elements of the critical infrastructure can be compromised by weaknesses in smaller entities to which they are technologically connected. Given this fact, it is critical for us to create a sustainably secure cyber ecosystem for all entities, large and small. Therefore, in the next phase of Framework development, we recommend that NIST work with interagency partners including the Department of Homeland Security (DHS), the Small Business Administration, and Sector Specific Agencies to better understand the cybersecurity and implementation challenges faced by organizations of all sizes, and consider ways to make the Framework more approachable for all organizations. NIST should prioritize understanding the issues confronting theses smaller entities and addressing their unique concerns and needs.

NIST should convene a dedicated process to explore long-term Framework governance options. Looking ahead to future governance is an issue NIST has consistently addressed since before the

Framework was even published. Yet at the same time, it is difficult to separate the Framework's early success from the NIST-convened process that created it, and NIST's stewardship since. As the primary users and consumers of the Framework, the private sector ultimately owns the Framework. But we shouldn't underestimate the continuing importance of NIST's role as convener, and custodian, of not only the Framework, but also the governance conversation. The smartest way to explore the future governance of the Framework is for NIST to convene focused discussions amongst stakeholders in the same thoughtful manner as that which produced the Framework itself.

One idea worth exploring in this regard is the creation of a governance advisory panel, comprised of experts from across industry, academia and other key stakeholder groups, tasked with developing and implementing a governance plan. To ensure the long-term success of the Framework, we believe an ongoing, formal strategic dialogue between NIST and key stakeholders could best position a future governance model that helps the Framework evolve in a way that is beneficial to all stakeholders.

One model such a panel could consider is what a non-profit organization taking over the long-term governance of the Framework would look like. While there is precedent for this -- a similar model was used for the Smart Grid and NSTIC IDESG efforts – those were primarily US efforts, and we should be careful to ensure that any model considered can scale globally.

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

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

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

Prioritize Addressing the Cybersecurity Roadmap Areas. All of the areas identified in the Roadmap for Improving Critical Infrastructure Cybersecurity, published concurrently with the Framework, are important to improving cybersecurity, and further research and /or industry-led standards development work in any of these areas should be prioritized. While the importance of continuing our collective research and standards development efforts in areas such as authentication and supply chain risk management cannot be overstated, however, this doesn't mean we should rush to include all roadmap topics into the next version of the Framework. We believe it is premature to incorporate topics lacking the requisite consensus-based, industry-led international standards and best practices in to the Framework. We encourage NIST to continue working with stakeholders to help promote development of standards in these areas, something we note NIST is already doing in other contexts, such as in the recently published “Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity,” which helpfully articulated the need to develop new standards in several important core areas of cybersecurity standardization.

In terms of prioritizing Roadmap areas for inclusion as Framework updates, two identified areas that strike us as ripe for inclusion in the next iteration of the Framework, are “Federal Agency Cybersecurity Alignment” and “International Aspects, Impacts, and Alignment.” We discuss our recommendations regarding both of these topics below.

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

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

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

White House cybersecurity coordinator Michael Daniel subsequently indicated the Administration was "beginning a process to identify federal regulations that were excessively burdensome, conflicting or ineffective."[2]

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

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

International Markets: Facilitating Data Flows and Driving Global Cybersecurity Standards

Cross-Border Data Flows and Cybersecurity. We commend the Commission for expanding its mandate to cover discussion of international markets, in acknowledgement of the global nature of our cybersecurity challenges, and the centrality of cross-border data flows to the modern digital economy.

A central element of ITI's global advocacy efforts involves helping governments understand the critical importance of cross-border data flows, not only to the ICT sector, but also to the global economy as a whole. Virtually every business that operates internationally relies instinctively on the free and near instantaneous movement of data across borders to enable their day-to-day business operations, from conducting research and development, to designing and manufacturing goods, to marketing and distributing products and services to their customers. U.S. and global ICT companies also have a long history of exchanging security-related information across borders with geographically-dispersed employees, users, customers, governments, and other stakeholders, which helps them better protect their own systems and maintain high levels of security for customer data, IP and the technology ecosystem as a whole.

Indeed, as well as facilitating secure business transactions amongst companies in disparate locales, global data flows are key to greater coordination and productivity for global companies, helping to secure the systems and networks that manage production schedules and Human Resource (HR) data, as

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

well as communicate internally with subsidiaries and employees in different geographies. The free flow of data across borders is also necessary to enable a seamless and secure Internet experience for hundreds of millions of citizens around the globe. Unfortunately, we can point to several examples of a troubling global trend of erecting barriers to the free movement of global data, both in the U.S. and abroad – for instance, Wassenaar Export controls related to intrusion detection software, the recent European court of Justice opinion invalidating the Safe Harbor transatlantic data transfer agreement, and forced localization measures in numerous countries.

Perhaps even more disturbing, the trend of impeding data flows generally, is contrary to the thrust of current U.S., and indeed global, cybersecurity policy, and threatens to undermine continued global cybersecurity progress.

To illustrate, as you know, late last year, Congress passed a bipartisan cybersecurity threat information sharing bill, the Cybersecurity Act of 2015.[3] The bill acknowledges that voluntary sharing of information regarding cyber threats, with appropriate privacy safeguards, is an integral component of improving our cybersecurity ecosystem, as it helps all stakeholders better protect and defend cyberspace. More specifically, Section 103 of CISA required the heads of various federal security agencies to jointly develop procedures to ensure the Federal Government maintains "a real-time sharing capability," And Section 105 directed the Attorney General and Secretary of Homeland Security to jointly develop policies and procedures to govern how the Federal Government receives and shares information about cyber threats, including via an automated real-time process (both of these tasks have already been completed). Section 203 of CISA requires the Department of Homeland Security, in coordination with industry and other stakeholders, to develop an automated capability for the timely sharing of cyber threat indicators and defensive measures. President Obama signed the law, which aligns with the Administration's consistent recognition of the critical importance of cross-border data flows and real-time information sharing in combatting security threats to the global ICT environment. For instance, also last year, President Obama issued Executive Order 13691,[4] which, among other things, states, "private companies, nonprofit organizations, executive departments and agencies, and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible."

All of these policy efforts are intended to spur the voluntary sharing of cyber threat information among and between businesses and government entities to improve cybersecurity, and all of these initiatives contemplate the sharing of cybersecurity threat information as inclusive of information related to vulnerabilities. Given that the overarching intention of these policy initiatives is to promote expedited sharing of threat information to improve cybersecurity, we are concerned that the Proposed Rule and the 2013 additions to the Wassenaar Arrangement could undermine this key principle and severely complicate the ability of companies in all sectors and government entities to share information in real-time to protect and enhance their security.

[3] Consolidated Appropriations Act, 2016, H.R. 2029, 114th Cong., Division N (2015).

[4] Exec. Order No. 13,691, 80 Fed. Reg. 9347 (February 20, 2015), *available at* https://www.federalregister.gov/articles/2015/02/20/2015-03714/promoting-private-sector-cybersecurity-information-sharing.

Implementation of the Wassenaar controls, however, would necessarily slow down the sharing of vulnerability information (both intra-company and between companies). In other words, because the Wassenaar controls are effectively erecting additional barriers to vulnerability sharing, it appears diametrically opposed to the goals of multiple cybersecurity policy initiatives recently advanced by U.S. government policymakers.

International Cybersecurity Framework Alignment Efforts. International Framework alignment is essential, and foundational to driving such alignment involves the global Framework promotion efforts of both industry and government. As a sector, we have supported organizations across the globe who are using the Framework as the basis to assess their actual cybersecurity risks. The Framework is gaining traction internationally, and familiarity is growing in multiple geographies. Notably, earlier this year, Italy adopted its own version of the Cybersecurity Framework. Further, international use of the Framework is gaining support in the following sectors: Financial, Electric Utilities, Water Utilities and Oil and Gas. Furthermore, the Framework is being used to establish security requirements and as a way to recommend threat mitigation controls and remediation. Promoting the Framework in its current form will help the US to sustain its leadership on cybersecurity around the world, and this will in turn help to further enhance the Framework's use within the United States.

To facilitate further global adoption, NIST and its Federal agency partners should promote the Framework approach with their global government partners. For example, the Department of State should reference the Framework in all of its global cybersecurity capacity-building efforts. Likewise, the White House should highlight the Framework in its strategic cybersecurity partnerships. International acceptance of industry-led, global cybersecurity standards will help drive even greater competition and innovation in the global marketplace.

NIST should also consider other mechanisms by which to expand the Framework approach. For example, given the increasing global acceptance of the Framework, we would support NIST exploring, with industry stakeholders, the opportunity for submitting the Framework as an international standard. This could be a valuable contribution to further harmonizing cybersecurity practices on a global scale. Today more than 80 countries are in the process of creating new cybersecurity regulations and there are myriad implementing requirements being considered. Adding the Framework as an international standard could help propagate a standards based approach globally.

Prioritizing global Framework outreach. Outreach to international audiences, including the sharing of best practices, should be significantly enhanced. It is particularly important that foreign governments who are carefully watching the Framework's development better understand its approach. Many governments around the globe are at pivotal points in their own cybersecurity policymaking—examples include the EU's Network and Information Security (NIS) Directive, which must be implemented by all 28 EU member states over the next 18 months, and cybersecurity policies and laws at different stages of development across Asia and Latin America. However, many foreign governments and audiences outside the U.S. generally still do not understand the Framework's voluntary, risk management approach or its rationale, and mistakenly believe NIST is writing new standards for the U.S. economy. Thus, international outreach that focuses on the facts underlying the Framework and the approach it embodies will continue to be essential. Conducting such outreach in local languages (e.g. with the assistance of our Embassies abroad) would be extremely helpful.

Driving Global Cybersecurity Standards. The global ICT industry is heavily invested in developing standards to address important challenges in security management. We urge the USG to continue taking a leadership role in promoting the adoption of industry-led, voluntary, globally recognized cybersecurity standards and best practices, to make the preservation and promotion of a global market a primary goal in any product assurance requirements, and avoid country-specific requirements. We also welcome and encourage all governments to participate in standards development activities, particularly in private fora and consortia. Governments might also consider greater action in their own (public sector) use of voluntary, globally accepted standards or generally accepted industry practices for cybersecurity risk management. Indeed, government leadership can demonstrate such standards' importance and may be necessary to overcome economic disincentives to adoption of standards that yield benefits to the network as a whole.

We applaud the USG for continuing to invest in global standards development (via the International Standardization Strategy). However, it's worth noting the purpose of furthering international cybersecurity standards is not for governments to turn around and mandate their adoption. From ITI's perspective, any effort to mandate minimum security standards is problematic, in that it is difficult for a minimum standards approach to allow for the flexibility for best security practices to evolve as technology advances, or to fully take into account the necessary risk management processes at the heart of cybersecurity. ITI thus strongly cautions all governments not to set compulsory security standards for the commercial market– whether they are standards vendors must follow as they build their products or services, or standards that would guide consumers when purchasing ICT products and services or conducting business with companies. Such an approach could encourage some firms to invest only in meeting static standards or best practices that are outmoded before they can even be published or cause others to divert scarce resources away from areas requiring greater investment towards lower priority areas. To maintain (rather than restrain) innovation and to prevent the development of single points of failure, any standards should be purely indicative, their use entirely voluntary, and should always allow organizations to adopt alternative solutions. Defining new, country-centric standards has many downsides as such insular standards may conflict with global standards currently in use, interfering with global interoperability.

Internet of Things: Avoiding Siloed Policymaking and Regulatory Approaches

The Commission should also be commended for adding the Internet of Things (IoT) to its mandate. While IoT is not new – since the Internet was invented, various devices have been connected and networked in attempts to improve convenience, functionality, and for many other purposes – all of these now hallmarks of IoT are increasingly achieving much greater success and occurring on a more pervasive scale. Indeed, the rapid growth of networked devices and Internet applications due to the availability of components, Internet service, and the technology that make Internet connection possible – whether we are talking about Smart Grid, Smart Cities, Connected Autos – have us fast headed toward an Internet of Everything. Given this, USG and other government bodies must look at the underlying technologies and assess where current authority, oversight, and regulation already exist. It should also seek to identify areas where government is approaching this correctly, and replicate that activity in other areas. There are a number of relevant policy areas where authorities already exist, where government is facilitating IoT development, and where industry is working with government to address new or evolving issues stemming from the IoT, including cybersecurity and related issues.

Cybersecurity and IoT. Significant activity continues to take place across both government agencies and the private sector in an effort to strengthen our cybersecurity, including for IoT. The interests of government agencies and industry are aligned in this arena in that both aim to minimize vulnerabilities and create networks, products, and devices that are as secure as possible. Consequently, much of the activity designed to enhance cybersecurity takes place in consultation and close collaboration with the private sector, and we strongly encourage that public-private partnership (PPP) approach to continue.

As mentioned previously, ITI's member companies are at the forefront of providing security solutions from the devices at the expanding network edge to the cloud, and across the network and IoT. With billions of additional devices coming online, ITI's companies ensure that security is embedded in IoT platforms at the outset of the manufacturing and design process for each new device that extends and expands the network. Security must be built into both hardware and software at the outset to ensure there are redundancies, to prevent intrusions, and to create secure and trusted IoT systems. Advances in hardware technology allow for security to be physically built into a system. For example, semiconductor manufacturers can design chips with built-in safeguards. Encryption, for instance, can be baked in at the chip level. Manufacturers can also prevent chips from being rewritten by designing fuses into chips. If a hacker attempts to access or rewrite the data, the fuse pops and prevents the data from being rewritten. Similarly, on the network side, devices communicating with the network will require a reliable level of service and connectivity, as well as high security to prevent unwanted intervention. New Internet protocol architectures are more adaptable and use advanced technologies to pervasively distribute security, treat individual users and devices with an appropriate level of performance and privacy based on their needs, and automate manual processes to improve scale and availability. Application programming interfaces (APIs) facilitate data interactions between edge devices, code modules, applications and backend IT systems. Organizations can leverage API management software to address security as an architectural challenge in the development of IoT applications.

USG stakeholders have a critical role to play in fostering security across the IoT; excellent groundwork has already been laid in this area and should be leveraged going forward. The tech sector has been partnering with the NIST for nearly three years developing and using the Framework, discussed at length earlier. It is instructive to recall the genesis of the Framework stems from Executive Order 13636,[5] issued in February 2013, which called for the government to partner with owners and operators of critical infrastructure to improve cybersecurity through the development and implementation of risk-based standards. Development occurred through a process of coordination and collaboration convened by NIST between the technology industry, others in private industry, and U.S. government partners.

[5] *See* White House, Executive Order 13636, Improving Critical Infrastructure Cyber Security, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

What resulted is a set of voluntary guidelines, best practices, and standards to help critical infrastructure, businesses, and other private and public actors to better manage cybersecurity risks. Taking a similar public-private partnership approach, NIST recently released a Framework for Cyber-Physical Systems[6] (the "CPS Framework"), also developed in partnership with industry, academic, and government experts. One of the key working groups in the cyber-physical systems project is focused on cybersecurity and privacy.[7]

ITI believes it is pivotal to continue to replicate this partnership approach in addressing IoT cybersecurity challenges. The NIST Framework provides an overarching structure, grounded in proven international standards and consensus best practices, to address organizational security across all critical infrastructure sectors, while providing adaptability and flexibility to meet the unique needs of each sector and address new threats. The CPS Framework provides additional technical details for building secure products for IOT, Smart Cities, Industrial Internet and other applications. On the flip side, viewing cybersecurity uniquely for each application, whether it be a home computer or an automobile, is inflexible and will leave industry less able to quickly and efficiently respond to new threats, potentially stifling innovation around security.

Perhaps of more concern is the potentially counterproductive precedent of creating siloed approaches to cybersecurity across different IT applications, as part of the IoT and beyond. As more aspects of our daily lives increasingly become digitized, and more "things" are indeed connected to the internet in order to make our lives richer and more efficient, surely we do not need to reinvent the wheel when it comes to security, as each of these applications or use cases gains prominence. At different stages of the recent past, policymakers have considered whether new regulatory regimes were needed to better secure critical infrastructure, the electric grid, cloud computing, or health IT, and in each instance, after close examination, the benefits of approaches grounded in voluntary, consensus-based international standards that can both promote innovation and preserve the promise of interoperability have carried the day. The alternative – a world in which we endeavor to separately regulate each new IT application or IoT vertical – is not realistically scalable, and simply unsustainable in an IoT world.

Another area in which the government can provide leadership is to make certain that efforts to improve cybersecurity leverage public-private partnerships and build upon existing initiatives and resource commitments. The IT industry, along with our peers in other industry sectors, leads and contributes to a range of significant public-private partnerships, including information sharing, analysis, and emergency response with governments and industry peers. Two key examples of public-private partnerships the government can prioritize to ensure greater coordination and collaboration across the government and industry are information sharing and analysis centers (ISACs), and sector coordinating councils (SCCs).

While ISACs across a number of industry sectors have been in existence for varying periods of time and thus have different experience levels in responding to threats and vulnerabilities, more mature ISACS such as the Information Technology ISAC (IT-ISAC) (formed in 2000 and operational since 2001), and the Financial Services ISAC (launched in 1999) have developed best practices for effectively receiving and

[6] *See* NIST CPS Draft Framework: http://www.cpspwg.org

[7] http://www.nist.gov/cps/cpswpg_security.cfm

distilling threat information and working with the groups' members. The ISACs are invaluable in helping address sector specific and cross-sectoral threats and vulnerabilities. For example, the IT-ISAC helped monitor and collaborate with its members on large-scale threats such as Conficker and the DNS Cache Poisoning Vulnerability. The IT-ISAC provided a forum for members to engage in collaborative analysis on those significant issues, and to draft and share analytical alerts with remediation suggestions that were shared with members, partner ISACs, and the public. Mirroring the growth of IOT, we now see new ISACs being formed, such as the Automotive ISAC (formed about a year ago), which can benefit from the experiences of the more established ISACs. For example, threats and vulnerabilities that the IT-ISAC may have encountered in other forms could manifest themselves within connected automotive applications such as those enabling in-car purchases, vehicle-to-vehicle communications, and auto communications with roads and highways. Close collaboration between the IT-ISAC and the Automotive ISAC could provide valuable lessons and solutions to new problems based on variations of issues that may have been faced by the technology sector in the past. The same may be true as other sectors that previously did not face vulnerabilities due to technology or software become increasingly connected to the network.

The SCCs are self-organized and self-governed councils enabling critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities related to cybersecurity. The SCCs coordinate and collaborate with their counterparts across the US government, primarily their sector-specific agencies and related Government Coordinating Councils (GCCs), to address and facilitate government collaboration on a wide range of critical infrastructure security and resilience policy and strategy issues. The U.S. IT industry formed and funds the IT Sector Coordinating Council (IT-SCC) to work closely with the Department of Homeland Security (DHS) to ensure better preparedness and coordination of critical infrastructure protection (CIP) initiatives impacting the IT Sector. Recently, as part of the revised National Infrastructure Protection Plan (NIPP), the IT-SCC collaborated with its GCC partners at DHS to develop and revise a Sector-Specific Plans (SSP) focusing on the unique operating conditions and evolving risk landscape impacting the sector. SCCs across 17 critical infrastructure sectors similarly completed revised SSPs in 2015.

Privacy and IoT. Given the projected exponential growth in the number of devices that will produce, and analyze, or transmit data, obvious questions around data privacy arise. Since one of the primary purposes of cybersecurity is to better secure such data, we briefly address the issue of IoT privacy here. At the outset, it is important to keep in mind that a significant amount of data will have no connection to a person or individual; for instance, industrial or commercial IoT applications will largely be used for diagnostic, logistic, or other performance-related purposes. Secondly, data that is de-identified or anonymized and aggregated do not raise the same privacy concerns as other collections and uses of data.

In applications where data on individuals is collected, the collection, use, sharing, and protection of such data are already subject to existing laws. For instance, IoT manufacturers fall within the jurisdiction of the Federal Trade Commission (FTC) and are thus subject to its unfair or deceptive acts or practices authority under Section 5 of the Federal Trade Commission Act. Grounded in Fair Information Practices

Principles (FIPPs), the FTC's approach to privacy helped enable the Internet to thrive and, as a consequence, ITI companies have been able to offer an expanding range of services and applications (including IoT applications), often times free or at a nominal expense to consumers. While all FIPPs protections may not be applicable in all instances and flexibility may be necessary for certain IoT applications,[8] the FTC has the expertise and authority to oversee privacy matters for the IoT. In fact, the FTC has taken action in this space and brought a settlement against TRENDnet Inc., a company that markets Internet enabled video cameras.[9] In that case, the company failed to implement reasonable security measures, resulting in transmission of live video feeds from consumers' homes on the Internet. Depending on the data collected and who the actors are, other statutory authorities may also be applicable to the IoT. For instance, health information is protected under both the Health Insurance Portability and Accountability (HIPAA) Act and the Health Information Technology for Economic and Clinical Health (HITECH) Act, while the Graham-Leach-Bliley (GLB) Act and the FTC's Safeguards Rule govern the protection of information held by financial institutions.

Global Standards and IoT. Many of the existing foundational elements that drove the development, evolution, and investment in the Internet ecosystem existing today will be necessary to fully realize the potential of the IoT. Adoption of global, consensus-based standards, discussed extensively above, is critical for providing the interoperability necessary for the IoT to thrive. As the IoT technology landscape comes into greater focus, various global, industry-led standards-setting organizations (SSOs) have formed technical and study groups to ascertain to what extent additional standards development is necessary, including for cybersecurity. These bodies are typically international in scope, drawing experts and participation from across the globe and across various industry sectors that will be impacted by and benefit from IoT. It is important for the Department of Commerce and, more generally, all governments to share their needs and requests with these SSOs and, when appropriate, to actively participate.

Federal agencies should actively consult with industry regarding when and where to invest their time and resources in support of IoT standardization. The USG should strongly encourage governments to focus their time and resources on participation in and supporting industry-led standardization activities. When multilateral organizations are determined to proceed anyway, the USG should strongly encourage them to allow full industry participation, and to look to existing or pending global standards before undertaking any activity to engage in standardization activities that may be duplicative of, or even conflict with, global industry-led IoT standards.

Cybersecurity Workforce: Building a National Competency

The Cyber Security National Action Plan (CNAP)takes important steps to reverse the cyber talent shortage with the inclusion of a $62 million increase to the President's Budget to bolster cybersecurity personnel programs. One specific proposed step is to establish the CyberCorps Reserve program, providing cyber education scholarships to Americans seeking to serve their country in the federal civilian government. Others include the development of a Cybersecurity Core Curriculum, an increase in the

[8] See ITI comments to FTC, in *In the Matter of the Internet of Things*; FTC Project No. P135405; January 9, 2014.
[9] See *In the Matter of TRENDnet Inc.*; FTC File No. 122 3090; September 11, 2013.

number of participating academic institutions in the NSA Centers for Academic Excellence in Information Assurance Education program, and an expansion of student loan forgiveness programs for cyber professionals joining the federal workforce.

These education and workforce investments, in particular, will make a vital down payment to help close the cybersecurity skills gaps in government and the private sector. With more than 209,000 cybersecurity jobs in the U.S. unfilled last year, and predictions of 1.5 million more cyber jobs than takers by 2019, ITI and ITAPS are committed to supporting the CNAP's cyber workforce efforts and expanding initiatives like the CyberCorps Reserve program. The CNAP is a great step forward, but to remedy our alarming cyber talent deficit, we must recruit more than a million Americans trained in cybersecurity and information assurance. Only the federal government can lead response recruiting effort on the scale required. By offering young STEM graduates immediate employment protecting government and other critical assets, the government could stand up a Cyber National Guard that would quickly produce a trained workforce with practical experience and security clearances. After serving their country for five years in the public sector, Cyber National Guard veterans would find private companies such as those in ITI eager to hire them – and pay them what they are worth.

Cybersecurity and Federal Acquisitions: Harmonizing Efforts Across the Federal Enterprise

The EO 13718 directs the Commission to provide recommendations to improve the federal government cyber posture through procurement. ITAPS and ITI support the Commission's efforts to examine how to strengthen federal agencies' cybersecurity postures as they relate to acquisition planning and contract administration. Improving and strengthening our nation's cyber posture is rightly a top priority for our government and changing how the federal government integrates security into its own acquisition processes will help improve the cyber resiliency of the United States.

As further articulated above, we share the goals and interests of the federal government on the issue of cybersecurity because the protection of our customers, brands, and intellectual property are essential components of our members' businesses.

ITI and ITAPS have provided many recommendations throughout the years through providing comments to rulemakings and guidance and participating in various government stakeholder groups. As we stated in our more expansive recommendations to this Administration in July 2015, [10] security is essential to the federal government mission and should no longer be treated and addressed in a patchwork, uncoordinated fashion. Allowing the furtherance of uncoordinated security approaches will simply continue the current model and perpetuate a security regime that is only as strong as the weakest link.

To illustrate the number of overlapping and potentially conflicting requirements contractors currently face, we share the following inventory of just some ongoing or recently finalized regulatory actions:

- National Institute of Standards and Technology (NIST) guidance on cybersecurity and the management of controlled unclassified information (SP 800-171) (Revision 1 pending)
- FAR Case 2015-037, Definition of Information Technology (pending)

[10] ITAPS letter to OPM, OMB, and National Security Staff dated 30 July 2015, Cyber-Security Task Force Recommendations

- FAR Case 2015-026, Contractor Use of Mandatory Sources of Supply in Service Contracts (pending)
- DFARS Case 2016-D025, Liability Protections when Reporting Cyber Incidents
- OMB's Circular A-130, “Managing Federal Information as a Strategic Resource” (7/28/2016)
- DoD, GSA & NASA Final FAR, “Basic Safeguarding of Contractor Information Systems” (May 2016)
- Department of Defense (DoD) rule on the safeguarding of unclassified controlled technical information and reporting of associated cyber incidents (Superseded)
- DoD’s Interim Final DFARS on Network Penetration Reporting and Contracting for Cloud Services (Revised Dec. 2015)
- OMB's Improving Cybersecurity Protections in Federal Acquisitions (August 2015, pending)
- NARA Controlled Unclassified Information Notice of Proposed Rulemaking (May 2015, pending)
- Department of Homeland Security (DHS) Class Deviation 15-01 Safeguarding of Sensitive Information
- Anticipated Federal Acquisition Regulations (FAR) clauses on these topics (along with the fact that the FAR does not currently address the existing regime)

We urge the Commission to recommend to the President that in order to develop an efficient and effective cybersecurity acquisition infrastructure, OMB should harmonize all federal cybersecurity acquisition efforts to ensure that they are applied consistently across the entire federal enterprise. Without such oversight, an array of new requirements, regulation and guidance will add further confusion for the acquisition community, increasing the compliance burden for both the government customer and the vendor community.

In the recently released OMB's Circular A-130, “Managing Federal Information as a Strategic Resource”, OMB directs agencies to “make use of adequate competition, analyze risks (including supply chain risks) associated with potential contractors and the products and services they provide, and allocate risk responsibility between the government and contractor when acquiring IT.” The guidance further instructs the Department of Commerce to evaluate new information technologies to assess their security vulnerabilities, with technical assistance from the Department of Defense (DoD) and the Department of Homeland Security (DHS). We recommend that the government use a risk-based approach to spur better security and help contractors implement the rules with which they must comply. Any proposed approaches assuming that risk is generated only in the product or service to be acquired and overlooks some of the most important identifiers of cyber risk, such as the criticality of the mission or program and the intended use of the goods and services acquired for the support of that mission or program.

Additionally, no plan to improve cybersecurity and resilience through acquisition can be expected to succeed without some assessment of the risks inherent in the various processes and practices that are or will be used by the government for acquisition. Some acquisition practices, like using the lowest priced if technical specifications are met, or lowest-priced, technically acceptable (LPTA), do not support effective risk mitigation practices, and in fact may actually increase risk. We believe that for a cyber acquisition plan to be successful, it is critical that such a risk assessment be conducted at the front end of the procurement.

ITI and ITAPS recommend that an approach built around a capability maturity model that factors in varying levels of company capability based on size and type of business model, and that is flexible and risk-based would be a good starting point. We urge the Commission to recommend that agencies use the NIST Cybersecurity Framework government-wide to help determine agencies cyber risks, and explore how the Framework could be applied in procurement.

ITI and ITAPS members are global companies with global supply chains that sell their products and services in an integrated global market. We have strong concerns regarding proposals requiring companies to give the federal government "on demand" access to their facilities. Particularly in a post-Snowden environment, such unfettered government access policies can have huge economic implications. Many IT companies are custodians of sensitive customer information from customers around the globe. These companies cannot allow for unnecessary government inspections to compromise their customers' (particularly foreign governments) data privacy. Such requirements have implications for many of the latest technological capabilities, including cloud services. The technical construct of multi-tenant clouds, where the government is but one of many customers, would preclude access proposals to conduct assessments of systems. In such instances, if companies allowed the government to access their systems, they could be violating the contractual requirements of other customers, including other U.S. government agency customers. We are further concerned that unfettered government access/assessment provisions of this type could expose our companies' intellectual property and data systems to other parties, including private vendors hired by governments to conduct assessments or the government itself entering our facilities. Provisions of this type could have the net effect of requiring any global commercial company that does business with the government to have a segregated IT system to ensure customer data privacy, thereby forcing it to incur significant additional costs and raise prices for the federal government to do business. We recommend that the Commission not move forward with any recommendations that would require companies to give the government access to IT company's backend systems.

In today's complex cybersecurity environment, organizations must take a multi-layered approach to data protection to better secure the government's critical assets and most sensitive data, leveraging not just encryption, or access management and perimeter security, but data-centric security as well. A key part of any multilayered cybersecurity strategy is "data-centric security," which consists of protecting the native file format itself; doing so ensures that data remains secure wherever it travels or is stored. Data security is a critical risk to the federal government and a major cybersecurity challenge as the USG is one of the largest holders on personally identifiable information (PII) as well as classified, sensitive and related critical information. This data is stored, often in legacy information systems, and transmitted by email or moved from location to location using portable storage devices. This reality increases the potential exposure of data to potential loss.

Recent White House cybersecurity policies (OMB Circular A-130, the CNAP, Cybersecurity Strategy and Implementation Plan – CSIP) and congressional legislation support the importance of protecting data by compelling federal agencies to implement capabilities to "protect high value assets and sensitive information" and to "encrypt or otherwise render indecipherable to unauthorized users the data…stored on or transiting agency information systems" within the next year. Section 406 of H.R.

2029, the Cybersecurity Act of 2015, includes “information security management practices” such as “digital rights management” as a capability that federal agencies must report on utilizing “to monitor and detect exfiltration and other threats.”   The recently revised OMB Circular A-130 also establishes minimum safeguarding of federal information requirements and best practices that the commercial and government cybersecurity enterprise should follow:

- *Implement data-level protection and access controls to ensure the security of and access to Federal Information;*
- *Continuously monitor, log, and audit the execution of information systems functions by privileged users to detects misuse and reduce risk from insider threats;*
- *Encrypt all FIPS 199 moderate-impact and high impact information at rest and in transit;*
- *Implement processes to support use of digital signatures for employees and contractors; and*
- *Implement a policy of separation of duties….to reduce risk of malicious activity without collusion*.

With respect to PII, protected health information (PHI), intellectual property (IP), Homeland Security information, or related critical government data, the threat to documents and high value digital assets is persistent, eminent and evolving. While no one technology is a silver bullet, data-centric security controls can help improve the USG’s and commercial industry’s cyber security posture, working together with other information security products and practices.

Today, contractors ensure that security and privacy controls of systems operated by them or on behalf of the federal government comply with NIST standards and guidelines and agency requirements. Understandable in the environment post OPM breach, the government is concerned about protecting federal systems and data. Depending on the agency, requirements can be very prescriptive. We urge the Commission to recommend that contractors should be able to propose alternative IT security controls other than those required by NIST if they demonstrably provide the same or higher levels of security. ITAPS members are global companies that use international standards to secure their products and services, so such flexibility should be emphasized instead of prescriptive measures.

Improving and strengthening our nation’s cyber posture is rightly a top priority for our government, and changing how the federal government integrates security into its own acquisitions process will help improve the cyber resiliency of the United States.

State and Local Government Cybersecurity: Prioritizing Federal Grant Funding

ITAPS has recently published a detailed cybersecurity best practices document aimed at improving state and local cybersecurity, which we submit with this filing (also available at a link here). Additionally, we would like to highlight the following two points:

Federal Grant Funding. It is important that state and local governments prioritize information security and utilize existing federal cybersecurity grant programs. The federal government must continue to allocate resources and expertise to state and local governments to ensure that the vast amount of personal identifiable information held by state governments is adequately protected and prioritized. Additionally, the federal government should further educational efforts provided to states and local governments on how to best utilize existing grant programs and how to take advantage of new opportunities.

Leverage Industry Recognized Standards. States should leverage industry recognized standards and existing technologically neutral international frameworks. Vulnerability reporting should be consistent across states so that they can be widely and quickly shared. State-by-state unique requirements should be avoided to prevent a balkanization of requirements that will impede international and interstate commerce.

CONCLUSION

ITI and ITAPS would like to again thank the Commission, as well as NIST, for demonstrating a commitment to utilizing transparent processes and partnering with the private sector to advance our shared cybersecurity goals. We would also like to commend the Administration for its willingness and eagerness to consistently engage with our companies and the ICT industry generally to determine how government and industry can best work together to improve cybersecurity, and one that we hope future Administrations, as well as governments globally, will embrace. The commitment to industry outreach is an excellent example of how effective public-private partnership processes can help to improve cybersecurity.

Given we are assured of a transition to a new Administration in 2017, it is hard to underestimate the importance of the Commission's mission – to provide a cybersecurity policy roadmap that ensures a seamless transition, and maximizes the value of the cybersecurity progress recently achieved by the Obama Administration (led by NIST) as well as Congress. While we won't recap all of our recommendations here, we will reiterate the importance of furthering risk-management and flexible approaches grounded in international standards that leverage public-private partnerships – all of which are hallmarks of the Cybersecurity Framework. We urge the next Administration to embrace the Framework, and hold up the Framework approach as a model that can help improve cybersecurity not only in the U.S., but globally.

ITI, ITAPS and our members look forward to continuing to work with the Commission, NIST and the present and future Administrations to further Framework development and the approach it embodies, and on other initiatives to improve our cybersecurity posture. Please continue to consider ITI and ITAPS as a resource on cybersecurity issues moving forward, and do not hesitate to contact us with any questions regarding this submission.

Sincerely,

John Miller
Vice President for Global Policy and Law
Cybersecurity and Privacy