Information Technology Industry Council
Leading Policy for the Innovation Economy

August 18, 2011

Mr. Jon Boyens
Senior Advisor
Computer Security Division
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 893
Gaithersburg, MD 20819

Via e-mail to: Securitygreenpaper@nist.gov

RE: Response to Cybersecurity, Innovation, and the Internet Economy Notice of Inquiry (Docket No. 110527305-1303-02)

Dear Mr. Boyens:

The Information Technology Industry Council (ITI) is pleased to provide the following comments on the Department of Commerce's (herein "Department") recently released "Cybersecurity, Innovation, and the Internet Economy" draft report (herein "Green Paper").

ITI is the premiere voice, advocate, and thought leader for the information and communications technology (ICT) industry. ITI's 50 members comprise the world's leading technology companies. As both producers and consumers of cybersecurity products and services, our members have extensive experience working with the U.S. Government—as well as governments around the world—on the critical issue of cybersecurity policy. As you are aware, the interests of industry and governments in increasing cybersecurity are fundamentally aligned.

ITI commends the Department's Internet Policy Task Force for its continued attention to the nexus of cybersecurity, innovation, and the Internet economy and for undertaking the challenging task of developing an initial proposal for "a new framework for addressing Internet security issues for companies outside of the orbit of critical infrastructure or key resources." We understand that the intent of the Green Paper is to stimulate further discussion by reporting on the Task Force's preliminary findings and continuing the consultation process that began in 2010. In this response, ITI will focus on certain questions raised in the Green Paper. ITI is uniquely positioned to provide useful and timely input on key topics, including those that benefit from our global perspective. Working closely with the U.S. Government, foreign governments, and domestic and foreign trade associations, ITI has been a leading player in addressing key cybersecurity policy concerns that have arisen over recent years as countries enact national cybersecurity policies that disrupt commerce and harm innovation. Further, our members are global companies. Most derive a substantial portion of their revenues from foreign markets and have extensive global supply chains. As a result, we have an acute

1101 K Street, NW • Suite 610 • Washington, DC 20005 • t: 202.737.8888 • f: 202.638.4922 • www.itic.org • @ITI_techtweets

understanding of the impact of governments' policies on cybersecurity innovation and of the need for U.S. policies to be consistent with – and drive – global norms.

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

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

We are pleased that many of the Green Paper's proposals reflect the approaches described in our Principles. We applaud the suggestions, many of which we highlight below, that follow an approach based on public-private partnerships, global cohesion, flexibility, and raising awareness. At the same time, in our responses we also have described how greater adherence to the Principles would significantly strengthen cybersecurity in the "Internet and Information Innovation Sector" I3S and we have proposed specific suggestions for how to accomplish that goal. We look forward to working with you address this important topic.

ITI's responses to proposals or questions raised in the Green Paper are below. The Department's proposals and/or questions are in bold.

II. Recommended Definition of Internet and Information Innovation Sector (I3S)

- **How should the I3S be defined? What kinds of entities should be included or excluded? How can its functions and services be clearly distinguished from critical infrastructure?**

We commend the Department's attempt to define an "Internet and Information Innovation Sector" (I3S) that would be out of the scope of "covered critical infrastructure" (CCI). Current proposals allow for CCI to be regulated under existing law or Administration policy or future proposals. We understand that the Department's goal of defining this sector is to provide clarity that the Administration does not consider portions of the information technology (IT) sector, including Internet-based services, to

[1] The IT Industry's Cybersecurity Principles for Industry and Government, found at http://www.itic.org/clientuploads/ITI - Cybersecurity Principles for Industry and Government - Final1.31.11.pdf
[2] See: What its electronic and information technology -- http://www.washington.edu/accessit/articles?106
[3] http://www.safecode.org/publications/SAFECode_Training0409.pdf

be CCI. We agree wholeheartedly with the importance of drawing a fine line between entities in those sectors of the economy whose functions and services are truly critical—and therefore whose failure would be catastrophic in terms of mass casualty event, a significant national security incident, or a catastrophic halt of economic markets—and entities in the IT sector whose products and services unquestionably support and enhance many other economic sectors (including CII entities) but for which failure in and of itself would not be equally catastrophic. As the Department appreciates, most networks and Internet-connected technologies are not critical infrastructure and should not be designated as such.

In response to the Department's request for comments on its proposed definition of the I3S in the Green Paper we offer the following thoughts. While we appreciate the Department's attempt to define our sector, and we understand the difficulty in doing so, we believe the proposed definition does not go far enough to comprehensively cover all of the IT hardware, software, and services companies that are part of the innovation economy that the Department has described. It is clear that the IT industry, including software and hardware, are part of the I3S; thus the Department's forthcoming White Paper and any statute should be clear that—in addition to the Internet and information services which are otherwise covered in the Green Paper—the IT industry, including software and hardware, are excluded from CCI. If there is some "IT product" used in the limited number of critical infrastructure assets (as we define below, those like a nuclear facility or dam the failure of which could lead to a mass casualty event, a significant national security incident, or a catastrophic halt of economic markets), such as a cyber-physical control system, only that product in that facility should be subject to any mandatory regime of that covered critical infrastructure.

To the extent that new critical infrastructure requirements are codified, the scope of the non-covered Internet and I3S should be codified using precise and commonly recognized terms. One definition we suggest to use is derived from the Clinger-Cohen Act set forth below.

Definition of Electronic and Information Technology. The Clinger-Cohen Act of 1996 (40 U.S.C. 1401(3)), also known as the Information Technology Management Reform Act, establishes a definition of information technology in Section 5002 of the Act that has since been cited in numerous other federal laws including the 1998 amendments to Section 508 of the Rehabilitation Act which defines "electronic and information technology" this way:[2]

- ***Electronic and information technology.*** *Includes information technology and any equipment or interconnected system or subsystem of equipment, that is used in the creation, conversion, or duplication of data or information. The term electronic and information technology includes, but is not limited to, telecommunications*

[2] See: What its electronic and information technology -- http://www.washington.edu/accessit/articles?106

products (such as telephones), information kiosks and transaction machines, World Wide Web sites, multimedia, and office equipment such as copiers and fax machines. The term does not include any equipment that contains embedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, are not information technology.

- ***Information technology**. Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term 'information technology' includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.*

Therefore, in addition to the Internet and information services the Department lists in the Green Paper, the IT industry, and software and hardware products, should be included the scope of I3S, including the 'information technology' and 'electronic information technology' definitions derived from the Clinger-Cohen Act—and excluded from the definition of CCI.

Without a more comprehensive definition of the I3S, we fear policymakers could extend proposed CCI regulatory structures beyond what is necessary to protect our nation's most critical systems to every system that connects to the Internet. Our proposed definition would help to focus resources where they are most needed and ensure minimal conflicts with other regulatory regimes. This definition also will help to ensure that these companies will continue to have the potential for growth, entrepreneurship, and vitalization of the economy.

- **What kinds of entities should be included or excluded? How can its functions and services be clearly distinguished from critical infrastructure?**

Any new CCI regulatory mandates should be focused solely on the specific cyber-physical entities that must be protected to keep Americans safe from catastrophic loss. Such entities would include those whose failure could lead to a mass casualty event, a significant national security incident, or a catastrophic halt of economic markets.

While the Administration's section-by-section analysis that accompanied its cybersecurity legislative proposal indicated the Administration's goal was for "only the most critical entities would be regulated under this title," we applaud the Commerce Department for its recognition that the definition contained in the legislative proposal was constructed too broadly and should not include I3S. Without additional clarity, such an

overly-broad scope could capture many unnecessary elements of the Internet economy and its customers and spread resources too thin, rather than focusing on the most critical facilities that we need to keep America safe (i.e., vital cyber-physical systems that control core critical infrastructure such as nuclear plants and dams, whose failure could result in mass casualties). Narrowing the definition would help focus government and industry resources—money, time and cyber-expertise—where they are most needed and ensure minimal conflicts with other regulatory regimes.

By contrast, ambiguity about what constitutes a CCI could lead to inefficient use of limited homeland security resources, and defer or delay other important investment decisions. For example, critical infrastructure operators need clear and stable definitions of asset criticality so they will know exactly what assets to protect, and how to appropriately invest in their protection. Otherwise, they risk protecting too many facilities, protecting the wrong facilities, or both.

- **Should I3S companies that also offer functions and services to CCI be treated differently than other members of the I3S?**

No. When I3S companies offer to CCI entities IT functions and services not specifically created for CCI these I3S companies should be treated the same as other I3S companies: they should not be regulated as CCI.

This question is an important one. An owner and operator of CCI can more effectively assess what IT product or service it needs for cybersecurity risk management than the I3S supplier of that product or service. Therefore, if a CCI entity purchases/uses an I3S vendor's product or service, the CII owner/operator, not the I3S vendor, is responsible for selecting the appropriate product/service to meet the CCI entity's cybersecurity needs as well as implementing, integrating, maintaining, and upgrading it. As a result, the I3S entity should not be considered CCI.

In recent years, it has become increasingly common for commercial off-the-shelf (COTS) hardware and software to be utilized even in CCI systems directly owned or operated by military and intelligence agencies. Experience has repeatedly illustrated that commercially available technology offers greater flexibility and innovation at a significantly lower cost than can be achieved through products and services specifically designed for civilian, military and intelligence applications. Products that are widely used often benefit from higher levels of security while delivering greater functionality and appreciable cost-savings.

This model would be broken—and the benefits lost—if COTS products and services could not be sold to the owners and operators of CCI unless they were engineered by companies that were subject to a separate set of cyber security frameworks. The result would be either that fewer companies would be qualified to sell to CCI customers or that products for sale to the general market might rise in cost due to the inclusion of security

features not relevant to customers that do not own or operate CCI. Instead, the current model, whereby the system owners are in the best position to understand their threat profiles and appetites for risk, must be retained.

Only in those unique cases where IT products and services are created specifically for CCI and those critical facilities that are vital to keeping America safe—e.g., cyber-physical and SCADA systems that control core critical infrastructure like nuclear plants and dams and whose failure could cause mass casualty events—should the I3S vendor be held responsible for the impact of an IT product/service breach or failure on the CCI in question and be held to any regulatory standards applicable to cybersecurity for that CCI. However, even in those cases we do not believe the IT vendor should itself be considered CCI.

An approach that affirms such a key distinction will help to ensure that a regulatory structure necessary to protect our nation's most critical systems is not extended to every system that connects to the Internet or beyond what is reasonable.

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

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

Policy Recommendation A1: The Department of Commerce should convene and facilitate members of the I3S to develop voluntary codes of conduct. Where subsectors (such as those with a large number of small businesses) lack the resources to establish their own codes of conduct, NIST may develop guidelines to help aid in bridging that gap. Additionally, the U.S. government should work internationally to advance codes of conduct in ways that are consistent with and/or influence and improve global norms and practices.

We agree that there is an important role for NIST to play in the area of promoting improved cyber security in the proposed I3S sector. We further agree that NIST is the appropriate agency to work on the development of cyber security technology and standards through its Cyber Security Division of the Information Technology Laboratory. However, it is imperative that NIST be adequately funded so that it has the necessary in-house expertise to do so and keep to a minimum the outsourcing to third parties of its standards work. NIST also must engage in an open and transparent process with industry in the process of developing any guidance for private industry.

We are concerned, however, about the concept of "nationally recognized approach to minimizing vulnerabilities." Efforts to promote the development of country-specific codes of conduct are likely to have unintended consequences. They could, for example,

embolden other countries to develop their own national requirements, standards, or codes of conduct.

It would be more productive and less troublesome for NIST to serve as a convener and participant in existing standards-setting efforts rather than for it to act as a leader or coordinator of national efforts. As noted below, it is certainly sensible to coordinate the U.S. Government's engagement in standards-setting bodies and NIST is best suited to this role. However, neither standards development nor the development of industry codes of conduct should be led by the U.S. Government. A more active role for NIST in standards development would send negative signals to other countries that seek to engage in top-down standards development practices.

Rather than for NIST to lead the development of codes of industry conduct, perhaps it could support and facilitate efforts by industry-led consortia to develop appropriate security frameworks and reference materials for use by I3S companies who are incentivized by the market to adopt better security practices. Such practices will ideally draw upon existing globally accepted, industry-led, voluntary, consensus-based standards. Examples of standards that could be drawn upon include the Common Criteria for Information Technology Security Evaluation (CC), an accepted U.S. and international standard for computer security certification intended to provide product assurance globally. The CC is both the International Organization for Standardization (ISO) standard and a mulilateral agreement among 26 countries including the United States, Japan, the UK, Australia, Germany, Korea, and India. There are many other industry-led, consensus-based security standards being developed by groups such as ISO that could also be drawn upon. Where relevant standards cannot be identified, we would suggest the development of a mechanism to allow for review and validation of generally accepted industry practices.

NIST also should consider promoting efforts of industry consortia aimed at improving the secure development of IT products and services. One example is the Software Assurance Forum for Excellence in Code (SAFECode), a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware, and services. SAFECode includes a framework that can be used by small, medium, and large enterprises to develop in-house corporate security training for software assurance.[3] Another industry initiative, known as the Building Security In Maturity Model (BSIMM) provides a starting point for considering what activities should be integrated into the software development process.[4]

NIST should continue to encourage important private sector work and coordinate with relevant Federal Agencies, the private sector, and universities to increase awareness of such industry initiatives among small and medium businesses.

[3] http://www.safecode.org/publications/SAFECode_Training0409.pdf
[4] http://bsimm2.com/index.php

NIST's leadership would also be particularly useful in supporting the development of industry-operated conformance test frameworks. In order for market forces to properly incentivize security improvements, it must be possible to effectively measure and understand which security efforts yield measurable results and at what cost. Again, this work could be accomplished through collaboration with industry-led consortia.

Regarding the recommendation for international work, ITI appreciates the Department's clear understanding that efforts to improve cybersecurity must take into account the global nature of cyberspace. This is consistent with ITI's Principle 2. As the Department is aware, cybersecurity approaches that differ dramatically by country—a policy patchwork—not only present potentially negative consequences for security, but also disrupt global commerce and ignore the borderless nature of the Internet. As the Department also is aware, any approaches the United States takes will be watched carefully, and perhaps emulated, by governments around the world. Thus, the U.S. Government has a strong responsibility to make sure any codes of conduct we promote are systems that would be equally beneficial if deployed globally.

The U.S. Government should, however, be cautious about conferring too much authority to the Federal Trade Commission (FTC) to bring civil law enforcement actions against companies who are suspected of being out of compliance with security standards or practices, a suggestion posited on p. 12 of the Green Paper. We have some specific concerns about the role of the FTC.

First, we are concerned as to whether the FTC has sufficient resources to develop the expertise necessary to determine whether or not companies are in compliance with codes, standards, or practices to which they might publicly ascribe. The model cited by the Department in the Green Paper has worked well with regard to privacy policies. Such polices are readily capable of interpretation by FTC staff, who have significant experience understanding what privacy promises are meaningful to consumers and the economic harms that can result from misuse of personally identifiable information. By contrast, questions about compliance with technical security standards and practices used to secure complex systems that are commonly used in the I3S are generally not the expertise of FTC staff. It may not be sensible to add this responsibility to the Commission without simultaneously providing them with additional staff and training—an outcome that is highly unlikely in the current budgetary climate.

Second, there is a vast difference between what entities can "promise" with regard to their privacy policies and their security practices. First, a privacy policy has a unique purpose: it states how an entity will treat personal information it receives from a customer. The customer then can decide whether to provide the entity with his/her personal information. Secondly, privacy policies tend to be somewhat static. Although they may be updated over time, we argue that updates tend to be relatively infrequent.

In contrast, effective security policies and practices are matched to an entity's particular cybersecurity threats, vulnerabilities and consequences, and change in tandem with changes in these variables. Thus, it is highly unlikely that any two entities will employ the exact same (or even demonstratively similar) security practices. To expect the FTC to discern whether practices are appropriate to a given situation seems unrealistic. Just as ITI stated in our response to the Administration's legislative proposal that having DHS regulate our sector could make us less secure, we also believe having the FTC try to enforce codes of conduct could lead to decreased security.

Although we do not believe that the FTC should have civil law enforcement oversight with regard to enforcing entities' stated security policies, we do believe it important that the public be better able to understand what security practices an entity is deploying so that the public can decide whether to patronize a particular entity or purchase its products or services. In such a case, market forces would ideally steer entities towards implementing the most effective security practices, for fear of losing customers.

We understand that facilitating such a marketplace that rewards "good security hygiene" was the intention of the Department's effort to identify certain cybersecurity standards, guidelines, and best practices for promotion (examples are in the Green Paper's Appendix B). According to the Department, these identified practices are ones about which the status of an entity's implementation/compliance is transparent and available to the public. For example, users can see whether an entity is using a secure browser (indicated by "https") or if they are implementing DNSSec.

- **How should the U.S. Government work internationally to advance codes of conduct in ways that are consistent with and/or influence and improve global norms and practices?**

See our answers below to the Policy Recommendation and questions in "D. ENSURING STANDARDS AND PRACTICES ARE GLOBAL."

Policy Recommendation A2: The Department of Commerce should work with other government, private sector, and non-government organizations to proactively promote keystone standards and practices.

- **Are the standards, practices, and guidelines detailed in Appendix B appropriate to consider as keystone efforts?**

ITI understands that the Department's long-term vision is for industry to develop and use effective cybersecurity codes of conduct based on overarching principles, performance measures, and detailed standards and practices. Because such an approach will take time, however, in the short term the Department seeks to pinpoint existing effective security standards, practices, and guidelines that have some degree of consensus or acceptance among security professionals and that could be more widely deployed voluntarily as a starting point to build better general industry practices and help to

improve America's cybersecurity posture. In response to the request for input as to which of the suggested standards, practices, and guidelines listed by the Department in Appendix B have the greatest potential in this regard, and which should be prioritized for the Department's promotion (on a voluntary basis), ITI has the following comments.

Overall, we agree with the goal of identifying some general security standards for which greater deployment can ultimately raise the bar for security and reduce pressure to regulate. Of the ones listed in Appendix B, useful options the Department may wish to prioritize are DNSSec and identity management and authentication standards and policies that will be developed under the National Strategy for Trusted Identities in Cyberspace (NSTIC).

DNSSec is and will continue to be critical in preventing web-based fraud, including problems such as domain name spoofing and hijacking. These are very important problems that deserve near-term attention and promotion of best practices within the I3S.

Identity management and authentication standards are critical to enhancing security on the Internet and to reducing cyber intrusions and other incidents. As the Department acknowledges in the Green Paper, these solutions are not deployed widely enough for a variety of reason. This led to the issuance of the NSTIC in April 2011 to help to bring together public and private sectors to develop an "identity ecosystem" of interoperable technology standards and policies. The Department should prioritize the establishment of the NSTIC and its work and then prioritize the promotion of NSTIC standards and policies widely. In particular, a federated identity standard should be promoted to address password hacking and "password chaos" that threatens Internet security. Of course, any standards developed should be market driven.

- **In what way should these standards, practices, and guidelines be promoted and through what mechanisms?**

These standards, practices, and guidelines should be promoted through public-private partnerships between government and all stakeholders. This approach will assist the range of cyberspace's stakeholders—consumers, businesses, and infrastructure owners and operators—in understanding and undertaking their important role in helping to address cybersecurity risks. ITI advocates a focus on user responsibility in our Principle 5. This approach, in addition to being the most effective, will send the right signals to our international trade partners—that we believe that public-private partnerships are the most effective and workable approaches to improving cybersecurity.

We further recommend that, rather than creating new mechanisms or partnerships, the U.S. Government should build on its existing sponsorship of the private sector-created and led National Cyber Security Alliance (www.staysafeoline.org), which is the leading security awareness public-private partnership in existence. Consistent with ITI's Principle 1, this would leverage existing industry initiatives.

- **Should the government play an active role in promoting these standards, practices, and guidelines? If so, in which areas should the government play more of a leading role? What should this role be?**

Yes, the government should play an active role through public-private partnerships, as noted above.

NIST, with its clear mission and expertise related to cybersecurity standards, guidelines, and best practices, is best suited to undertake this role, should be designated the lead agency to do so, and should receive adequate funding to maintain and augment the needed in-house expertise. Although NIST can and should partner with other agencies such as DHS as needed in promoting cybersecurity standards, guidelines, and best practices for the I3S sector, a lack of clear guidance as to NIST's leadership in this area could potentially risk an interagency struggle over this responsibility. This would result in resources being misdirected away from actually helping industry to improve cybersecurity risk management. It also would send conflicting messages to industry regarding which government agency is responsible for this important task.

A critical role the U.S. Government should play in promoting the standards, practices, and guidelines is to work closely in collaboration with international partners. Although the private sector can and does work on a cross-border basis to develop and implement important voluntary cybersecurity standards, guidelines, and best practices, the U.S. Government has relationships with governments around the world. All governments seek to increase cybersecurity within their economies, and many, including the United States, are grappling with the best ways to do so without stifling commerce and trade. As the Department is well aware, cyberspace is a global and interconnected system that spans geographic borders and traverses national jurisdictions. Hence, a globally consistent approach to improving cybersecurity is essential to avoid balkanizing the global market with conflicting approaches, guidance, or priorities among governments. This approach is enshrined in our Principle 2.

As noted above, a U.S. Government priority on coordinating globally will send the right signals to our trading partners. Conversely, any steps the U.S. Government takes with regard to unilaterally promoting domestic specific standards or best practices could be met with similar activities by other governments.

One area where the U.S. Government should consider greater unilateral action is in its own use of voluntary, globally accepted standards or generally accepted industry practices. The federal government may be best able to demonstrate the importance of a global, voluntary security standard or practice by using it. Such actions may do more to ensure greater adoption than would be possible through efforts to highlight individual companies—or even groups of companies—who have implemented them. Indeed, U.S. Government leadership may be necessary to overcome economic disincentives to

adoption of standards that yield benefits to the network as a whole rather than primarily to the entity adopting the standard.[5]

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

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

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

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

Policy Recommendation A4: The Department of Commerce, in concert with other agencies and the private sector, should work to improve and augment conformance-based assurance models for their IT systems.

As noted above, the development of better measures—and consequently more information about what security practices yield measurable results—will naturally lead to a better understanding of risks associated with the failure to adopt specific security measures. This will, in turn, naturally bring about the result that the Department advocates—voluntary assertions by I3S companies that they are in compliance with specific standards and practices.

The development of better measures will also lead to better mechanisms for assessing compliance with promises to adhere to standards and practices, which will allow the market to efficiently attach a price to the failure to actually implement those security

---

[5] See Allan Friedman, Brookings Economic and Policy Frameworks for Cybersecurity Risks, July 21, 2011 at p. 10. "Even adding new security components can be difficult if it requires individual decisions. Many security innovations, such as DNSSEC, yield their benefits to the entire network. There is little incentive to be the early adopter, since network security products often do not improve overall security until other users adopt them. Indeed, products that are not subject to network externalities and offer benefits to the early adopters, such as SSH and IPsec, are more likely to succeed and diffuse quickly (Ozment and Schechter, 2006)."

policies, practices, and procedures that are actually effective. Absent such measures, the market will continue to labor under lack of meaningful information about what security measures actually work.[6] Accordingly, the Department should focus more efforts on addressing the market forces that serve as a disincentive to adoption of better security as opposed to attempting to develop new incentives.

B. BUILDING INCENTIVES FOR I3S

Policy Recommendation B1: The Department of Commerce and industry should continue to explore and identify incentives to encourage I3S to adopt voluntary cybersecurity best practices.

- **What are the right incentives to gain adoption of best practices? What are the right incentives to ensure that the voluntary codes of conduct that develop from best practices are sufficiently robust? What are the right incentives to ensure that codes of conduct, once introduced, are updated promptly to address evolving threats and other changes in the security environment?**

As noted above, the U.S. Government should put its emphasis on developing better measures to enable transparent assessment of whether particular security standards—including both international standards and globally recognized, industry-led, voluntary, consensus-based standards—and generally accepted industry practices produce measurable security improvements and the costs associated with those improvements. The development of these measures will naturally lead the market to assess the efficacy of particular practices and to put a price on adoption, or failure to adopt, effective security measures.

- **How can liability structures and insurance be used as incentives to protect the I3S?**

As the Department rightly points out, liabilty fears can hinder entities' ability to voluntarily adopt cybersecurity best practices. ITI strongly commended the Administration, in its May 2011 legislative proposal, for taking steps to address private entities' liability concerns related to voluntary sharing of threat, vulnerability, or incident information with the federal government in order to gain advice or assistance to better protect or remediate their own information systems, as well as to assist with federal

[6] See Allan Friedman, Brookings Economic and Policy Frameworks for Cybersecurity Risks, July 21, 2011 at p. 10. [T]he market for security is fraught with information asymmetries that prevent optimal decision-making. Anderson (2001) helped launch the field of economics of information security by observing that the market for security products paralleled Ackerloff's (1970) market for lemons, or bad used-cars. Buyers are unwilling to pay for what they cannot measure. Producers are therefore unwilling to invest in producing security, but will still assert the security of their products. Like an untrustworthy used car market, bad security products will drive out good ones.

efforts to protect federal information infrastructure.[7] The Administration had introduced proposals to limit liability in those situations, although ITI noted in our comments our concern that the liability protections were too vague to adequately incentivize the level of information sharing desired and needed for purposes of strong cyber security. We suggest that any efforts to address liability clearly extend liability protection not only to the disclosure of any information but to the resulting impact from exploitation of a reported vulnerability.

- **Should federal procurement play any role in creating incentives for the I3S? If so, how? If not, why not?**

It can play a role, if done right.

It is acceptable for procurement policies to specify security objectives, as long as the decisions regarding how to meet those objectives (such as what technologies to use or how or where to build them) are left up to the I3S vendor that would like to sell to a federal agency. However, it is essential that federal procurement policy in no way include any mandates regarding how the IT industry designs and develops its products, including how I3S companies run their supply chain. Such an approach would be seriously detrimental to the mitigation of cybersecurity risks in U.S. federal IT systems and networks by making products less, not more, secure. This approach also could lead to de facto technology mandates on the U.S. IT industry and disrupt the innovation process of U.S. IT companies, as well as the global business model of build-once, sell globally and adherence to global standards.

In addition, a U.S. Federal Government procurement approach that mandates how or where IT products are built could embolden other governments to do the same. This would undermine the interoperability and security of networks globally and also have huge negative commercial implications for U.S companies.

Policy Recommendation B2a: Congress should enact into law a commercial data security breach framework for electronic records that includes notification provisions, encourages companies to implement strict data security protocols, and allows states to build upon the framework in defined ways. The legislation should track the effective protections that have emerged from state security breach notification laws and policies.

In June 2011 ITI released a set of Data Breach Notification Principles that describe what we would like to see in a national framework. In short, ITI strongly supports efforts to establish a commonsense, uniform national standard to protect the security of consumers' most sensitive personal information from identity theft. We support a national data

[7] See Department of Homeland Security Cybersecurity Authority and Information Sharing Act Sections 245 and 246: "Voluntary disclosure of cybersecurity information and limits on liability."

breach notification process that is consumer-driven, simple, and promotes information security best practices. A federal standard should preempt existing state laws, be technology neutral, and limit notification requirements to those instances when a consumer's personal information has been compromised.

ITI favors the enactment of a single, uniform, federal commercial data security breach legislation, which includes notification provisions and which encourages the development of data security protocols. It is sensible to model such legislation upon those provisions in state laws that have proven effective. However, federal legislation must preempt any state law that would result in the application of inconsistent or conflicting requirements upon companies holding commercial data. It is reasonable to expect that states should have the ability to enforce the federal requirements. However, there should be no private right of action as they are likely to yield only expensive litigation and potentially conflicting results without leading to measurable security improvements.

To avoid confusing consumers with notices when there is little or no appreciable risk of harm, notification requirements must be risk-based. For example, when data are not in a form that presents a significant risk of identity theft—e.g., because they do not contain personally identifiable information or because they have been rendered unreadable—notice should not be required.

Notification requirements should be held in abeyance when requested by law enforcement or national security officials. Reporting requirements to the government should be limited to those situations where there has been some indication of criminal activity. Such processes should be simplified to allow for reporting to either the Federal Bureau of Investigations or the United States Secret Service.

Policy Recommendation B2b: The Department of Commerce should urge the I3S to voluntarily disclose their cybersecurity plans where such disclosure can be used as a means to increase accountability, and where disclosure of those plans are not already required.

We understand the purpose of this proposal is to allow interested parties, such as shareholders, to understand the preparedness of a given entity and raise accountability that an entity is establishing and following plans to address cybersecurity issues. However, we believe publishing security plans detailing how an I3S would be protected could jeopardize our national and economic security. The Administration itself, in its May 2011 cybersecurity legislative proposal, acknowledged this fact by proposing that covered entities publish high-level summaries of their plans, not the plans themselves.[8]

However, as ITI also commented on the May 2011 legislative proposal, even this

[8] See Cybersecurity Regulatory Framework for Covered Critical Infrastructure Act Section 7 (b), "Public disclosure of cybersecurity plans and certifications."

approach has its drawbacks. A plan that is summarized at too high a level provides no value to those who will try to assess it. Moreover, publication of even high-level summaries introduces new risks, which must be balanced against the likelihood that such summaries will offer interested parties significant insights into the risks associated with the operation of I3S entities. While I3S companies may wish to voluntarily publish this information as a market differentiator, we fear U.S. Government urging to do so would become a paperwork exercise that does not improve, and could substantially threaten, cybersecurity.

There are other ways for companies to demonstrate accountability, namely through the use of global standards and practices. Voluntary attestation to standards and practices can drive accountability and obviate the need for the disclosure of plans that could hold potentially sensitive information.

In addition, as ITI previously commented, we do not favor mandatory inclusion of plan information in SEC filings for publicly traded companies. The Administration's cybersecurity legislative proposal would require publicly traded companies to make a series of certifications regarding the fact that a plan has been developed, that it is has been evaluated by third party, and the results of that evaluation. We are concerned that this approach confuses the policy goal of ensuring the protection of critical infrastructure with the policy goal of protecting investors. Public companies work diligently on disclosures that present a balanced picture of the strategic and operational risks and opportunities companies face. Prescriptive disclosure can erode a company's ability to present this balanced picture, based on its specific facts and circumstances.

- **Should an entity's customers, patients, clients, etc. receive information regarding the entity's compliance with certain standards and codes of conduct?**

We understand that one reason the Department suggested in the Green Paper that the U.S. Government promote the use within the I3S of the eight cybersecurity standards, guidelines, and best practices listed in Appendix B is that information is already publically available as to whether entities are in compliance with these standards. Thus, we do not think any additional guidance/encouragement to disclose compliance is necessary.

As a general principle, required disclosures from private sector companies to their customers should be limited to those instances where the information is meaningful and actionable. Any other approach would cause I3S companies to expend enormous amounts upon the delivery of notices, which would quickly overwhelm the public with information that they cannot use. Moreover, here the potential exists for widespread publication of information about whether a particular system or asset is in compliance with a specific security standard or practice is likely to introduce significant new security risks.

- **Would it be more appropriate for some types of companies within the I3S be required to create security plans and disclose them to a government agency or to the public? If so, should such disclosure be limited to where I3S services or functions impact certain areas of the covered critical infrastructure?**

No, for the same reasons mentioned above. Again, notice to the public is not likely to be usable and actionable. In addition, widespread availability of this information will introduce significant new security risks. As noted above, companies that have customers who own and operate systems or assets that may someday be designated as CCI should not have separate obligations from the rest of the I3S. Such requirements would significantly limit the pool of vendors serving the owners and operators of CCI. Limiting selection in such a manner would hamper their ability to tap into the cost-savings, efficiency, and innovations—including innovations in security functionality—that the competitive commercial market offers.

Policy Recommendation B3: The Department of Commerce should work with other agencies, organizations, and other relevant entities of the I3S to build and/or improve upon existing public-private partnerships that can help promote information sharing.

We agree with and support the Department's commitment to promoting private-public sector collaboration to facilitate information sharing. This acknowledges the value of U.S. public-private partnerships, which have been a cornerstone of U.S. policy for decades. We also agree with the emphasis on using existing public-private partnerships, rather than building new ones. These points adhere to ITI's Principle 1 (leveraging public-private partnerships and industry initiatives).

ITI continues to urge the federal government to better share specific, actionable information on cyber threats with private sector actors so that the latter can react more quickly and sufficiently. Examples of actionable information include actual instances of deliberate corruption of the supply chain or specific, actionable threat intelligence related to network-based intrusion or activity.

- **What are the barriers to information sharing between the I3S and government agencies with cybersecurity authorities and among I3S entities? How can they be overcome?**

Many private-sector entities would like to be able to voluntarily disclose threat, vulnerability, or incident information to the federal government in order to gain advice or assistance to better protect or remediate their own information systems, as well as to assist with federal efforts to protect federal information infrastructure. Some entities have found useful information-sharing mechanisms but there is general consensus that gaps remain. In addition, certain factors preclude many private-sector entities from

disclosing such information. These include a valid fear of legal repercussions, concerns about security of the data once shared, and the lack of a uniform and trusted mechanism that supports a useful information-sharing and -analysis partnership. We have some suggestions to address these factors.

First, we strongly commended the Administration, in its May 2011 legislative proposal, for taking steps to address liability concerns by introducing proposals to limit liability when such information is voluntarily shared.[9] However, as ITI noted in our comments on that proposal, we are concerned that these proposed liability protections contain some ambiguities. Therefore, these protections may not adequately incentivize the level of information sharing desired and needed for purposes of strong cyber security. Specifically, the proposed language in Section 246 does not expressly address liability in connection with an actual vulnerability or incident. Thus, if a private-sector entity were to notify the federal government of a network vulnerability, and that vulnerability became known, the entity would be at risk of legal action. We suggest any legislation or regulation in this regard more clearly extend liability protection not only to the disclosure of the information but to the resulting impact from exploitation of a reported vulnerability. Such clarification could lead to the desired goal of more extensive information sharing that can improve cybersecurity. As a general matter, any proposal should have very strong liability protections for private sector entities cooperating with the U.S. Government, and should extend to all forms of cooperation.

Second, we urge the Administration to ensure the implementation of a uniform and trusted information-sharing mechanism. Rather than working to create a new voluntary information sharing architecture, we suggest that we use and strengthen existing information sharing and analysis centers (ISACs), such as the IT-ISAC. Many entities in the I3S already leverage the IT-ISAC to report incidents and their resolutions to facilitate the development of lessons learned, aggregation, and trending data. DHS is already a beneficiary of that information sharing and analysis. Some options could be for the ISACs to create redacted versions of their work products for the I3S sector and/or encouraging appropriate I3S entities to join the IT-ISAC.

- **Do current liability structures create a disincentive to participate in information sharing or other best practice efforts?**

Yes. See our comments above.

C. EDUCATION AND RESEARCH

Policy Recommendation C1: The Department of Commerce should work across government and with the private sector to build a stronger understanding (at both

[9] See Department of Homeland Security Cybersecurity Authority and Information Sharing Act Sections 245 and 246: "Voluntary disclosure of cybersecurity information and limits on liability."

the firm and at the macro-economic level) of the costs of cyber threats and the benefits of greater security to the I3S.

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

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

- **What new or increased efforts should the Department of Commerce undertake to facilitate cybersecurity education?**

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

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

We have three specific recommendations that can help to achieve the goal described above. First, accreditation bodies for universities' computer science and related (e.g., control systems) curricula should have primary responsibility for demanding that security concepts be embedded in all computer science-related classes. The Department should encourage accreditation bodies to demand such changes in these curricula. Second, the U.S. government should tie grant monies—of all kinds, not just computer related—to

computer science curricula change in universities. Although this is not the purview of the Commerce Department, the Department should encourage the responsible federal agencies in this regard. Third, the Department should bring interested and knowledgeable stakeholders together to create security examples that can be included in computer science and related textbooks, and work with the Department of Education to encourage textbook publishers to incorporate security examples and sections into all computer science textbooks. Professors would then have something to teach to.

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

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

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

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

We agree. ITI also recommends that the Department seek out industry participation in developing strategies and setting priorities related the cybersecurity-related R&D. Further, the Department should promote public-private partnerships for cybersecurity

R&D, particularly partnerships that include a multi-disciplinary approach involving the IT hardware, software, and networking sectors.

D. ENSURING STANDARDS AND PRACTICES ARE GLOBAL

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

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

We believe NIST should continue to serve as the federal coordinator for international collaboration and cooperation to promote cybersecurity standards, generally accepted industry practices, and guidelines. Moreover, NIST's role as federal coordinator—both internally and externally—for the federal government's cybersecurity standards activities must be reaffirmed and strengthened. The National Technology Transfer and Advancement Act of 1995 (NTTAA) says that NIST is "to coordinate the use by Federal agencies of private sector standards, emphasizing where possible the use of standards developed by private, consensus organizations" … and "to coordinate Federal, State, and local technical standards activities and conformity assessment activities, with private sector technical standards activities and conformity assessment activities, with the goal of eliminating unnecessary duplication and complexity in the development and promulgation of conformity assessment requirements and measures."[10] There are currently a number of federal agencies involved in the development and representation of U.S. Government policy positions in international cybersecurity standards work. While all of this work is critical and the agencies' varying perspectives and expertise is important, at the end of the day to be effective this work must be coordinated interagency to ensure a common U.S. Government position that is in the best interest of U.S. industry. NIST has been assigned, and should play, that coordinating role.

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

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

- NIST: NIST develops standards and guides for securing non-national security Federal information systems. It defines minimum security requirements for federally held information and for information systems. NIST is also a primary contributor and member of the NITRD program, leading R&D in computer forensics tool testing, seamless mobility, trustworthy information systems, information security automation, combinatorial testing, next generation access control, and Internet infrastructure protection. NIST also is responsible for the National Software Reference Library, National Vulnerability Database, and Security Content Automation Protocol. NIST identifies methods and metrics for assessing the effectiveness of security requirements; evaluates private sector security policies for potential federal agency use; and provides general cybersecurity technical support and assistance to the private sector and federal agencies.
- NTIA: Over the past two decades, NTIA, in its role as principal adviser to the President on telecommunications and information policies, has worked closely with other parts of government on broadband deployment, Internet policy development, securing the Internet namespace, and other issues.
- BIS: BIS advances U.S. national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership.
- ITA: ITA strengthens the competitiveness of U.S. industry, promotes trade and investment, and ensures fair trade through the rigorous enforcement of our trade laws and agreements. ITA works to improve the global business environment and helps U.S. organizations compete at home and abroad. ITA promotes the commercial/business angle—informed by U.S. competitiveness interests—to U.S. Government cybersecurity policies.

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

The involvement of ITA is particularly critical to helping to promote global approaches related to cybersecurity standards and best practices and thus something on which we would like to elaborate. As the Department is aware, a growing number of governments

are enacting cybersecurity-related[11] laws, regulations, certification systems and other requirements, covering both government and commercial markets,[12] which purport to protect national security and economic interests. In many cases, these requirements (such as forced technology transfer or technology mandates) present obstacles to U.S. companies conducting business in those markets, are often inconsistent with generally accepted norms, standards, and best practices, and in several cases may actually violate international trade obligations. Moreover, such requirements rarely provide better security and in many cases may weaken security and disrupt global commerce. Foreign governments' cybersecurity-related policies and regulations that deviate from global approaches are becoming a top trade concern of the U.S. high-tech industry. Fortunately, this importance is reflected in the growing number of Administration officials from various Departments who are aware of and devote resources to these issues.

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

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

We have the following suggestions regarding how the U.S. Government can best do this work. ITI provided many of these suggestions in our September 20, 2010 response to the

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

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

Department's Cybersecurity, Innovation, and the Internet Economy Notice of Inquiry (Docket No. 100721305-0305-01).

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

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

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

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

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

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

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

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

Conclusion

ITI would like to again thank the Department's Internet Policy Task Force for its continued attention to the nexus of cybersecurity, innovation, and the Internet economy and for putting together its initial proposal for a new framework for addressing Internet security issues for the I3S sector. ITI also would like to commend the Department for having integrated so much of the input it has received from industry over the past year on this topic, and for its willingness and eagerness to consistently engage with our companies and the IT industry generally on how government and industry can work together to improve cybersecurity. The Department's commitment to industry outreach in this regard is an excellent example of the effective public-private partnerships that are essential to improving cybersecurity.

We hope that our responses to the important questions raised in the Department's Green Paper are helpful and will receive due consideration. We are available at any time to elaborate on our comments and our suggestions. ITI and its members look forward to continuing to work with the Department and the Administration generally to improve

America's cybersecurity posture. Please continue to consider ITI a resource on cybersecurity issues moving forward.

Thank you very much for your consideration.

Sincerely,

Dean C. Garfield
President & CEO