1615 H Street, NW
Washington, DC 20062-2000
Tel: 202/463-3100
Fax: 202/463-3177
E-mail: abeauchesne@uschamber.com

U.S. Chamber of Commerce
www.uschamber.com

August 15, 2011

Ann Beauchesne
Vice President
National Security & Emergency Preparedness Department

Via e-mail: SecurityGreenPaper@nist.gov

Jon Boyens
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 893
Gaithersburg, MD 20819

Re: "Cybersecurity, Innovation, and the Internet Economy" Green Paper (Docket No. 110527305-1303-02)

Dear Mr. Boyens:

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than three million businesses and organizations of every size, sector, and region, greatly appreciates the effort the Department of Commerce ("Department") has put into writing its new green paper entitled, "Cybersecurity, Innovation, and the Internet Economy."

The Chamber applauds the Department for proposing the idea of a *voluntary* cybersecurity framework for an "Internet and Information Innovation Sector" (I3S) that falls outside of traditional U.S. critical infrastructure. The green paper covers a wealth of promising topics for discussion and debate as well as a lengthy list of questions. Our comments provided below are meant to supplement the Chamber's July 29 letter to the Department. We have not attempted to answer every question. Instead, we have focused on defining the I3S; promoting the adoption of industry-led, global standards; and encouraging improved information sharing among and between businesses and the government.

1. Defining the Internet and Information Innovation Sector (I3S)

The Department asks stakeholders to help define the I3S. Below, the Chamber supports the Department's proposal for voluntary adherence to cybersecurity standards and practices across all sectors of the economy. The Department correctly recognizes that the non-critical I3S is distinct from the nation's 18 critical infrastructures. Going further, the I3S certainly does not have the same level of operational criticality that would cause them to be deemed "covered" critical infrastructure under a new Administration legislative proposal. As such, the green paper's voluntary approach would need to be carefully harmonized with any new regulatory construct for covered critical infrastructure to avoid conflicts (e.g., regulatory creep).

1.1 Voluntary, Public-Private Approaches to Cybersecurity are an Optimal Way Forward

The Chamber is enthusiastic about the Department's emphasis on a voluntary framework consisting of public policies and private-sector-led standards and best practices that could help decrease cybersecurity risks and improve the overall posture of I3S companies. We maintain that voluntary, public-private approaches to cybersecurity — regardless of sector — are more productive than ones that impose prescriptive mandates on industry.[1] Layering new regulations on critical infrastructure will not only harm public-private partnerships, but they will cost businesses substantial sums (on top of what they are already devoting to security), and not necessarily improve national security.

1.2 The I3S is Distinct from Critical Infrastructure

The Chamber supports the Department's efforts in attempting to establish a new "sector," explicitly recognizing that not all Internet technologies and services should be viewed as critical infrastructure. The reasoning behind a non-critical I3S is sound. Homeland Security Presidential Directive (HSPD-7), which deals with "Critical Infrastructure Identification, Prioritization, and Protection," directs the government to focus on protecting and securing critical infrastructure and key resources that could be exploited to cause (among other outcomes) "catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction." In contrast, I3S technologies, even if incapacitated, exploited, or destroyed, are unlikely to cause a mass casualty event or threaten national security.[2]

The Department should consider broadening the scope of the I3S to include more of the information technology (IT) sector, such as hardware and software manufacturers, to make it separate from covered critical infrastructure.[3] The green paper states that the I3S includes functions and services that create or utilize the Internet or networking services and have large potential for growth, entrepreneurship, and vitalization of the economy, but would fall outside the classification of critical infrastructure as defined by existing law and Administration policy.

[1] The Chamber believes that a robust, public-private approach to cybersecurity policymaking is the preferred and ultimately successful method that the Department should adopt. The Chamber's *Internet Security Essentials for Business*, found at www.uschamber.com/cybersecurity (pp. 30-34), highlights the positive initiatives of five sectors — banking, chemical, communications, electric, and IT — to guard their businesses from interruption, prevent the loss of data, and protect public safety.

[2] HSPD-7 uses the definition of "critical infrastructure" contained in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e)); www.dhs.gov/xabout/laws/gc_1214597989952.shtm#0.

[3] See, for example, definition of the IT sector at www.it-scc.org/documents/itscc/ITSCC_Bylaws_November_2008.pdf, pp. 1-2.

Further, the green paper argues that business models may differ, but the following functions and services are included in the Department's conception of the I3S:

- provision of information services and content;
- facilitation of the wide variety of transactional services available through the Internet as an intermediary;
- storage and hosting of publicly accessible content; and
- support of users' access to content or transaction activities, including, but not limited to application, browser, social network, and search providers.

Ultimately, policymakers will need to be clear and concise about the I3S's scope in order to avoid fragmented and unpredictable rules that would stifle innovation, the free flow of information, and online commerce. To the extent that the definition of covered critical infrastructure is carefully crafted and narrowly tailored in legislation, the scope of the I3S should also be codified using precise and commonly recognized terms such as "Internet," "information services," and "electronic and information technology," previously defined by Congress and adopted by agency policies or rules.

1.3 Voluntary Codes of Conduct for I3S and Any New Requirements for Covered Infrastructure Warrant Careful Harmonization

The green paper states that the Administration is promoting cybersecurity legislation that would "catalyze the development of norms for practices of entities that maintain our critical infrastructure." In the proposed regulatory legislation, the Department of Homeland Security (DHS) and sector-specific agencies would identify "covered entities using the established criteria and input from the federal government, state, and local governments and the private sector." Based on communications with Chamber members, and industry broadly, the predominant view is that the "established criteria" for determining what entity may be covered is incredibly vague. The Chamber has serious concerns with elements of the Administration's cybersecurity legislative proposal for regulating critical infrastructure. Yet, looking down the road, the Chamber recognizes that any new regulatory construct for covered critical infrastructure will need be to be carefully harmonized with the green paper's voluntary approach to achieve compatibility and avoid conflicts.

The Department of Commerce will need to be mindful, which the green paper clearly recognizes, of how the scope of the I3S meshes with the National Infrastructure Protection Plan and the Administration's proposed cybersecurity regime for covered critical infrastructure. For example, if the I3S is defined broadly, it is conceivable that I3S providers whose customers own/operate covered critical infrastructure might be held, instead, to prescriptive security standards rather than to the voluntary practices proposed in the green paper. It is unclear how I3S companies will be viewed by federal officials if they provide I3S products or services commercially that span non-covered and covered critical infrastructure.[4] Moreover, it is far from

[4] If an I3S company is designated, even in part, as U.S. critical infrastructure, it could have at least two impacts globally: Other countries may similarly deem the I3S company critical infrastructure, bringing unwanted regulation. Or, it could bring the company increased scrutiny because U.S. laws may be perceived as inconsistent with, or

clear how DHS will treat the Department's voluntary codes of conduct, should an I3S business wind up being identified as an owner/operator of covered critical infrastructure through the regulatory process.[5]

Any new regulatory mandates on covered critical infrastructure should be focused solely on the specific cyber-physical entities that must be protected to keep Americans safe and secure from catastrophic loss or disruption. 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. The Chamber believes that the list of potentially covered critical infrastructure needs to be defined in legislation as narrowly as possible. One the one hand, the Chamber is concerned about a cybersecurity regulatory program that is massive, costly, and unproductive. On the other hand, one of the biggest obstacles to improving cybersecurity is that too many entities will be deemed "critical" or supportive of "critical" entities. Not all systems or assets are equally critical (or the definition of what is considered critical changes over time). Not all data is equally critical. Designating broad swathes of systems as covered critical infrastructure will unintentionally diminish our ability to secure what truly *is* critical, given that resources — time, money, and, particularly, skilled cyber experts — are always in limited supply.

2. Supporting Flexible, Self-Regulation vs. Prescriptive FTC Mandates

The Administration should be scrupulous to avoid creating a voluntary program of cybersecurity practices and guidelines, only to have it subsumed by a regulatory regime — security does not lend itself to one-size-fits-all standards of conduct because each business's "critical assets" are different, each network is different, and the threats each business faces are different. For example, the green paper states that once these codes have been developed "and companies have committed to [following] them, relevant law enforcement agencies, such as Federal Trade Commission (FTC) and State Attorneys General, could enforce them, eventually leading to norms of behavior promoting trust in the consumer marketplace." Yet, automatically connecting codes of conduct to an enforcement regime will undermine the very nature of the self-regulatory structure as well as the public-private partnership.

Through the use of self-regulatory regimes, the Chamber supports the development of voluntary codes of conduct that enable continued flexibility in rules that can evolve with new technologies and business models. Self-regulation is an effective method of protecting consumers (e.g., privacy) because the regulatory process is often incapable of responding rapidly to market developments — including changes in consumer preferences and concerns — as well as advances in technology. Entities that will have to comply with these codes of conduct should

contrary to, foreign rules. Some U.S. cloud computing providers face added scrutiny abroad because the PATRIOT Act is viewed as giving inadequate protection to data in the United States, even though there is little negative impact on, say, individuals' privacy.

[5] Appendix B of the green paper seems to define the "codes of conduct" that the Department envisions for improving cybersecurity, but this is not a commonly used security term of art among security practitioners. The Department should clarify the term's usage and what its impact on business innovation and security will be. The codes may be appropriate is some environments, but in other places they may not be.

be responsible for their creation because it goes against the notion of self-regulation if these policies are actually developed and imposed on industry by the government. Uncorrected violations will be reported to the appropriate government agencies.

3. Promoting the Adoption of Industry-Led, Global Standards

The green paper asks for businesses' views on the standards, practices, and guidelines that the government should promote. The Chamber views cybersecurity as a global issue important to governments and businesses and encourage the U.S. government to pursue the development and enhancement of cybersecurity standards through engaging global standards bodies and foreign governments.

Businesses have been involved in developing internationally accepted cybersecurity standards, best practices, and international assurance programs for several years. Cybersecurity standards are routinely written and updated through open and transparent standards-development processes and organizations, such as the International Organization for Standardization (ISO), and processes. These efforts are global by design and scope and include active engagement by people from business enterprises and governments who are typically developers, consumers, and evaluators of IT products, and who have actual and relevant experience in designing, building, and securing systems. Applying relevant experience to standards development means the difference between workable, feasible standards and expensive certification schemes that may not be effective, or that may unintentionally weaken security by treating all threats as equal, all risks as equal, and all systems as equivalent.

Business and government entities voluntarily adopt international standards, practices, and assurance programs that best match their unique needs, operational plans, and cultural or regulatory environments. International standards-development processes are widely embraced by experienced practitioners who value the openness and credibility that these standards processes afford participants from multiple countries. Effective policies for improving U.S. and global cybersecurity products and practices must leverage the existing international standards-setting bodies.

National governments should resist the urge to develop, mandate, or even favor, a particular country-specific standard or standards. Among the upsides of an international approach to standards setting, international practices and requirements have the benefit of a global peer-review process. Further, the interoperability of security practices and technologies across multiple countries allows for an organization's limited resources to be more efficiently directed toward cybersecurity rather than encumbered by myriad national standards and mandates.

This is not to say that U.S.-specific standards that are voluntary and consensus based (e.g., American National Standards via American National Standards Institute-accredited standards-setting organizations) are inappropriate. Domestically driven standards must reflect and acknowledge the global environment and should be developed to leverage or harmonize the existing international standards — or drive them. The Chamber encourages the Commerce Department to take at least three actions:

- The U.S. government, through entities such as the National Institute of Standards and Technology (NIST), should take the lead in promoting the adoption of international cybersecurity standards and best practices developed by industry-led and/or public-private standards-development bodies.

- The federal government should collaborate with the private sector to implement, improve, and expand the Common Criteria for Information Technology Security Evaluation, generally known as the Common Criteria, which is the primary international standard (ISO 15408) for computer product assurance security certification. This international standard is recognized under a multilateral agreement (Common Criteria Recognition Arrangement) by more than 20 countries. Common Criteria is preferred by many in industry to a hodgepodge of country-specific standards, rules, and required actions that could unintentionally balkanize cyberspace and security or put industries' intellectual property at risk due to requirements for direct access to designs, source code, and other core IP.

- NIST should continue to build its capacity to engage in international standards-setting efforts that are industry led. NIST may find it useful to leverage its resources by participating first at the national level, and then through that participation becoming a much more effective representative of the voluntary, industry-driven position at the international level.

In sum, the Chamber encourages the Department to recognize the ubiquitous nature of cyberspace, which recognizes no borders. Efforts to enhance cybersecurity should be rooted in internationally accepted standards, best practices, and international assurance programs. The U.S. government, in partnership with the private sector, should push against the initiatives of foreign governments that would mandate cybersecurity standards and requirements that are not compatible with international practices. International standards, the *Cyberspace Policy Review* concludes, are critical to the security and vitality of our digital infrastructure.[6]

4. Encouraging Information Sharing through Greater Confidentiality, Limitations on Liability

A major theme of the green paper centers on improving public-private partnerships, such as removing barriers to information sharing between the I3S and government agencies. The Chamber is encouraged by a provision (section 245) of the Administration's cybersecurity legislative proposal that addresses the voluntary disclosure of cybersecurity information. It states that state and local governments and private entities that lawfully intercept, acquire, or obtain any "communication, record, or other information" may disclose that information to government officials (i.e., DHS officials in this case of the White House plan) if the information

[6] www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

will protect a network from cyber threats or help mitigate them. DHS, in turn, may share this information with other federal departments and agencies as well as with the private sector. While this proposed section seems consistent with many information-sharing practices among the information sharing and analysis centers (ISACs), the proposal should include additional language providing confidentiality to parties, including the I3S, who voluntarily share information.

Further, the green paper asks if current liability structures create a disincentive for participating in information sharing or other best-practice efforts. The Chamber views positively a related provision (section 246) that provides liability protections for private sector entities that, in good faith, disclose certain communications or other information or provide assistance to government officials. Policymakers should extend liability protections limitations to information that is given to ISACs from members of the I3S and the private sector generally.[7]

5. Flagging a Correction to the Green Paper

The Chamber wants to correct an unintentional error that was made in the green paper. Under a section of the paper (pp. 27-28) entitled "Using security disclosure as an incentive," its authors suggest that the Chamber's September 20, 2010, letter to the Department of Commerce supports greater regulation for companies to disclose data breaches. The Chamber does not support regulating businesses in the context of cybersecurity. Instead, we argued that policymakers often seek greater regulation for companies to supply cybersecurity as a public good (national defense). The Chamber noted that incentives would prove more productive than regulation. An excerpt of the Chamber's original September 2010 comments is provided below for more clarity and context:

> **An Incentives Framework for Evolving Cyber-Risk Options and Cybersecurity Best Practices**
>
> The Chamber encourages policymakers to incorporate more "carrots" and fewer "sticks" into measures to improve national cybersecurity. In an era of state-based and nontraditional threats to our economy and society, cybersecurity is an area in desperate need for incentives. Today, many policymakers emphasize the importance of individual business and sector preparedness, which the Chamber supports, but what they also seek is greater regulation to supply cybersecurity as a *public* good. It has been noted that "[c]ompanies have little incentive to spend on national defense as they bear all of the cost but do not reap all of the return. National defense is a public good. We should not expect companies, which must earn a profit to survive, to supply this good in adequate amounts."[8]
>
> Rather than regulate to compel business behavior, policymakers should incentivize the private sector to meet our shared national security and public safety requirements. Incentives are necessary to bridge the gap between what's in a company's interest to secure (based on risk) and what's in the interest of the country. The Chamber agrees with the *Cyberspace Policy Review*, which states that economic incentives and adjustments to liability considerations ought to be

[7] More on sections 245 and 246 can be found at http://democrats.senate.gov/pdfs/WH-cyber-general-authorities.pdf.

[8] Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency*, December 8, 2008, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf, p. 50.

explored. Models for liability protection include the “Support Anti-terrorism by Fostering Effective Technologies Act of 2002”, or SAFETY Act, and the “Year 2000 (Y2K) Readiness and Responsibility Act of 1999.” Congress should consider legal protections for entities that certify compliance with cybersecurity performance standards. Also, the Cross Sector Cyber Security Working Group is developing a package of incentives that Congress and the administration should study when developing new policy proposals.

In closing, the Chamber welcomes the Department of Commerce’s new green paper entitled, “Cybersecurity, Innovation, and the Internet Economy.” It represents a positive step forward in strengthening our national and economic security. We greatly appreciate having additional time to provide feedback, and we look forward to continuing to work with the Department to help advance its efforts.

Sincerely,

Ann Beauchesne

Ann Beauchesne