

August 1, 2011

Mr. Jon Boyens
National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive
Mail Stop 893
Gaithersburg, MD 20819

VIA EMAIL: SecurityGreenPaper@nist.gov

Dear Mr. Boyens and the Internet Policy Task Force:

TechAmerica welcomes the opportunity to provide these comments to the Department of Commerce (“the Department”) in response to its Green Paper on Cybersecurity, Innovation, and The Internet Economy. TechAmerica’s members have a vested interest in the success and future of the Internet, and we are pleased to engage in this important, on-going dialogue. TechAmerica is pleased to make these preliminary comments in this letter, and we will provide additional supplemental input in an expeditious manner based on our collective deliberations that we believe will contribute to the process going forward.

TechAmerica is the leading voice for the U.S. technology industry, which is the driving force behind productivity growth and jobs creation in the United States and the foundation for the global innovation economy. Representing approximately 1,000 member companies of all sizes from the public and commercial sectors of the economy, TechAmerica is the industry’s largest advocacy organization and is dedicated to helping members’ top and bottom lines. It is also the technology industry’s only grassroots-to-global advocacy network, with offices in state capitals around the United States, Washington, D.C., Europe (Brussels) and Asia (Beijing). TechAmerica was formed by the merger of the American Electronics Association (AeA), the Cyber Security Industry Alliance (CSIA), the Information Technology Association of America (ITAA) and the Government Electronics and Information Association (GEIA).

TechAmerica’s members include: manufacturers and suppliers of broadband networks and equipment; consumer electronics companies; ICT hardware companies; software and application providers; systems integrators; Internet and e-commerce companies; Internet service providers; information technology government contractors; and information technology consulting and sourcing companies. TechAmerica welcomes this opportunity to provide the Department’s Internet Policy Task Force with a viewpoint shared by such a diverse membership.

TechAmerica commends the Department’s Internet Task Force for engaging the process of examining the impact of public policy in the Internet age, and we have participated in all the Task Force proceedings, including privacy, global free flow of information, and intellectual property, as well as this effort on cybersecurity. The cybersecurity Green Paper puts forth an intriguing proposal for the designation of an Internet industry in the Internet and Information Innovation Sector (“I3S”) to reflect the innovation occurring in the information economy. We particularly

appreciate that recognition, as the technology industry is ever innovating and driving new products and services into the market faster than we have ever seen before.

The Green Paper also reflects today's reality that the technology industry is a provider of products and services to all manner of sectors. The nature of that symbiotic relationship means that while it is important to define parameters that designate one sector or another, it requires thoughtful deliberation and stakeholder input. We appreciate the Green Paper's discussion in that regard.

We do note that the new sector designation raises additional questions we would like to share for further exploration and collaboration. The definition of the sector as proposed in the paper, while illustrative, does not reflect the full scope of the sector that supports the information and innovation economy. We suggest that a more effective definition for the I3S could be guided by the definition of the Information Technology Sector in the National Infrastructure Protection Plan (NIPP), as follows:

- Domain Name System (DNS) root and Generic Top Level Domain (GTLN) operators
- Internet Service Providers (ISPs)
- Internet backbone providers
- Internet portal and email providers
- Networking hardware companies (e.g. fiber-optics makers and line acceleration hardware manufacturers) and other hardware manufacturers (e.g. PC and server manufacturers and information storage)
- Software companies
- Security services vendors
- Communications companies that characterize themselves as having an IT role
- IT edge and core service providers
- IT System integrators

We look forward to continued discussions on the definition of the I3S.

As further discussions continue, we must collaboratively explore the relationship between the "I3S" as defined as non-covered critical infrastructure and other considerations for the implications for innovation and the industry. For example, what is the relation with those functions and/or services that may be subjected to regulatory schema? How can we provide for predictability and clarity of the I3S designation vis-à-vis regulatory efforts? How can we clarify the responsibilities of the providers of I3S and users of I3S, and what is the role of contracts in that process? What are the implications for product designs and service offerings as they innovate and evolve in the future? How can we address the evolving nature of functions and services, particularly considering its evolving criticality of the use over time? We commend these questions to the dialogue and look forward to our continued engagement in deliberating them.

Further, the Green Paper calls for the I3S Sector to participate in the development and adoption of voluntary codes of conduct to bolster cybersecurity. Due to the dynamic nature of the industry, as well as that of the threats we face in cyberspace, TechAmerica believes that a voluntary approach that reflects that dynamism can contribute to cybersecurity if it encompasses elements of risk management and public-private partnership. Importantly, risk management efforts and a framework for public-private partnership are already well underway in the NIPP, and we encourage that any new processes for collective activity reflect that existing framework and the work within it. Once again, we suggest that the on-going dialogue address new questions arising from the proposal, such as whether the voluntary approach seeks to address improvements to general cybersecurity concerns or "the most serious threats" as posed in the paper's set of questions. Also, we look forward to providing more input on a productive process for determining the voluntary codes of conduct and the development of effective incentives for greater adoption throughout the industry.

Finally, we propose that there may some aspects of a sector designation and its participation in a voluntary code of conduct regime that are not addressed in the paper that would be valuable in the on-going dialogue. First, some existing best practices and standards in this space are not in the paper that would be useful, including (but not limited to) a description of the need for risk management practices in this ever evolving and dynamic environment. Second, existing programs could be bolstered to help meet the needs articulated in the paper, such as the NIPP (as already mentioned above), the international standards making bodies including the International Organization for Standardization (ISO), the role of Common Criteria for Information Technology Security Evaluation, the National Initiative for Cybersecurity Education (NICE), among others.

Thank you again for the opportunity to provide comment to the Green Paper and for the Department's efforts to engage stakeholders to further the Internet and information economy. As indicated, TechAmerica will provide additional input in the near term to contribute to the deliberation and collaboration on this important matter. As they arise, we welcome any opportunity to discuss the proposals in the Green Paper further with the Internet Task Force.

Sincerely,

A handwritten signature in black ink, appearing to read "Liesyl I. Franz". The signature is fluid and cursive, with the first name being the most prominent.

Liesyl I. Franz
Vice President, Cybersecurity and Global Public Policy