Software & Information
Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095
SIIA

Comments of the

Software & Information Industry Association

on the

Department of Commerce Green Paper:

Cybersecurity, Innovation and the Internet Economy

August 1, 2011

Thank you for leading this effort to craft a new framework to address internet security issues for companies outside the orbit of critical infrastructure, and for the opportunity to provide comments on the Green Paper on Cybersecurity, Innovation and the Internet Economy (Green Paper).

The Software & Information Industry Association (SIIA) is the principal trade association of the software and digital information industry, with more than 500 members that develop and market software and electronic content for business, education, consumers and the Internet. As leaders in the global market for software and information products and services, many SIIA members provide products and services that protect businesses, consumers and the public sector from cyber-attacks, viruses, and a wide range of online security threats.

I. Introduction

As a key component of the global digital economy, the software and digital information industries contribute greatly to U.S. economic growth and job production, represent a disproportionate share of U.S. global trade and influence and transform business models and user experiences across all sectors of the economy.

While innovation in these sectors is helping the U.S. continue as a global leader, there is little room for complacency. The threat of cyber attacks is evolving and becoming more dangerous and more adaptable to defenses. Sustaining the significant economic and job gains delivered by the software and information industries—and realizing new growth opportunities both in the United States and around the world—will depend on the ability to protect the security of consumers, businesses and the Internet infrastructure.

To that end, SIIA shares the goal of achieving the appropriate security framework to enable global interconnected ICT services to continue driving substantial commerce and economic growth across the globe.

SIIA and its members are dedicated to maintaining and expanding the partnership between the private sector and the government to address our nation's cyber security challenges, and we have spent much time over the last several years focusing on these critical issues, working closely with Administration officials and Congressional leaders toward the mutual goal of strengthening public sector networks and data security practices.

At the heart of the Green Paper is an effort to help define the roles of the Government and the private sector in combating this threat, protecting systems and networks that support the infrastructure that drives the Nation's economy. SIIA strongly supports the Department's approach of looking towards voluntary codes of conduct for an innovative sector such as the Internet and Information Innovation Sector (I3S). We believe this is the right approach to addressing the increasing cybersecurity challenges.

The most critical element of achieving these goals is to resist an approach that is overly-prescriptive, where mandates would have the adverse effect of slowing the development of standards in the private sector, or the unintended effect of putting U.S. companies at a disadvantage to their counterparts around the world. The Green Paper's proposed light-touch approach provides the necessary flexibility to keep up with rapid technological developments, pertaining to both threats and protections. This approach could help provide for a better security framework than a regulatory model could possibly achieve in covering a broad, rapidly-evolving cross-section of industry.

II. Definition

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?

While the primary purpose of the Green Paper is to discuss an area that is outside of the critical infrastructure segment, and to bolster security in this area, this exercise can also help to appropriately define the critical framework of what is "covered critical infrastructure" (CCI), and it can help to avoid confusion and appropriately allocate resources where they are most needed.

Most ICT networks and Internet connected technologies are <u>not</u> critical infrastructure and should not be designated as such. While increasing internet connectivity has led to myriad devices potentially being affected by cyber attacks, cybersecurity policy should not sweep all IT companies or their customers into the same regulatory basket as the most critical systems. The result of this approach would be to stifle innovation and create an impediment to enhancing cybersecurity.

Further the Internet infrastructure is constantly evolving and functions that in the early stages of Internet evolution would have been consider critical (due to issues of single points of failure, etc.) are now no longer critical to normal Internet function. Increased resiliency is constantly being built into the system and as such actions and players themselves are becoming increasingly less critical largely due to private-sector innovation.

A related proposal from the Administration, the Cybersecurity Legislative Proposal, leaves the critical infrastructure concept undefined. The definition provided in the draft legislation is both vague and overly-broad, taking the approach that almost everything could be considered critical as a way of keeping the definition open and flexible. But this could have dangerous consequences as it threatens regulation against an enormous swath of the IT sector and takes away private sector-led innovation efforts. As drafted, such an overly-broad scope is likely to capture many unnecessary elements of the I3S. To the extent the Department of Commerce's process helps to define what is not critical infrastructure, that is an incredibly useful exercise and one that could clear up much of the confusion within the space.

So, while the main goal in defining the I3S is to help explore the greatest threats and best practices to this vital sector of the economy, it also has the effect of clarifying more precisely the entities that must be protected to keep Americans safe from catastrophic loss. Such entities would include those whose failure could lead to mass casualties or a significant threat to national security.

We also urge the Commerce Department to articulate a mechanism whereby the definition of I3S services and functions can be integrated into the legislative proposals on cybersecurity to ensure that the I3S services and functions are not included in the definition of "covered critical infrastructure."

Is Commerce's focus on an Internet and Information Innovation Sector the right one to target the most serious cybersecurity threats to the Nation's economic and social well-being related to non-critical infrastructure?

The Department's focus on the I3S is a laudable objective, and a productive step towards helping to enhance awareness and preparedness by the entities that comprise this critical sector of the U.S. economy. So, while SIIA concurs that this sector should indeed be at the core of any effort to "target the most serious cybersecurity threats to the Nation's economic and social well-being related to non-critical infrastructure," it is imperative to consider how this effort would intersect with the highest priority of focusing on the protection of our Nation's critical infrastructure.

Given the potential for serious harm associated with cyber attacks to CCI, efforts should not be undertaken that would have the effect of draining resources or attention from that effort.

Should I3S companies that also offer functions and services to covered critical infrastructure be treated differently than other members of the I3S?

The intersection of CCI and I3S is a very complex, but important one, and SIIA commends the Department for exploring this intersection. SIIA does not believe that companies that also offer functions and services to CCI should be treated differently than other members of the I3S.

As a practical matter, only the entity that is characterized as CCI understands the operating risk environment it faces, and each such entity needs to be responsible for selecting the appropriate product or service to meet the its cybersecurity needs. In some cases, commercial off-the-shelf (COTS) products and services are sufficient for the needs of CCI entities, and in others, custom products and services are essential.

Many I3S providers are in the business of providing both types of solutions to a wide range of customers, including both CCI entities and non-CCI entities. Therefore, the most efficient approach to reach the desired level of security is to focus on the CCI entity, the party that is ultimately responsible for identify, implementing, and maintaining the appropriate technology.

One concern with the definition of "covered critical infrastructure," is that it could be interpreted to mean that an entire company is covered critical infrastructure simply because some of its services or functions are. In this regard it is crucial to ensure that only those services or functions that create the most sever risk are covered, and that other aspects of a company's operations are not included.

III. Development of and Promotion of Voluntary Codes of Conduct

Policy Recommendation A1:
The Department of Commerce should convene and facilitate members of the I3S to develop voluntary codes of conduct

Language in the Green Paper suggests the need for voluntary standards, and there is a significant focus on the creation of incentives for businesses that we address in the next section. However, other references in the Green Paper suggest the creation of a regulatory regime. It is imperative that this effort be a voluntary effort, geared primarily towards the goal of continually developing and updating best practices.

In addition to convening stakeholders and helping to develop best practices and codes of conduct, the Green Paper proposes that the U.S. Government work to promote these, make sure they are known, and lead efforts to keep them current. Indeed, this is a very substantial undertaking that should not be underestimated. Given the speed of technological advancement, including both technology to protect against threats as well as that used to pose them, keeping best practices and codes of conduct current will prove to be a substantial challenge.

While the involvement of the Department, and the Federal Government more broadly, is welcome to achieve mutual security goals, industry needs to retain the flexibility to experiment and act quickly to achieve the greatest level of security. A regime that cannot keep up with technological evolution would be the worst possible outcome.

What is the best way to solicit and incorporate the views of small and medium businesses into the process to develop codes?

The Green Paper, in recognizing that a large number of small businesses lack the resources to establish their own codes of conduct, suggests that NIST may develop guidelines to help aid in bridging that gap. However, the NIST-led effort may pose challenges to the laudable objective. That is, NIST's increasing reliance on outside vendors to lead security standards initiatives could have the undesired outcome of leadership by entities driving these efforts with the incentive to favor their particular products or business models, rather than seeking to achieve the greatest level of security. If NIST is going to play a leadership role in this area, it is critical that the agency be given the sufficient authority, resources and direction to sufficiently lead the effort, rather than outsourcing it.

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?

SIIA agrees that 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. At the heart of this should be promoting a global approach to cybersecurity that recognizes the global nature of interconnected systems and seeks international consensus standards that avoid fragmented and unpredictable national requirements.

IV. Improving and Modernizing Security Assurance

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

SIIA disagrees with a conclusion in the Green Paper that the "Common Criteria" are insufficiently flexible for a rapidly changing marketplace. On the contrary, having generally accepted methodology is critical. SIIA urges the Department, and the Administration, to avoid establishing any new, prescriptive supply chain or software assurance scheme that would establish the Government as a leader in the process of developing technology, or that would create a U.S.-centric standard. A U.S. Government-established security standard would conflict with the proven security regime that has long been the foundation of our effective national security strategy, with the likely outcome of impeding the use of commercially-developed technology and retarding the continued development of federal information security.

While the common criteria approach is very sound, there is strong support for continuing to reform and improve this approach. Specifically, the National Information Assurance Partnership (NIAP) is currently leading a collaborative effort with industry leaders to reform Common Criteria, an effort that promises to increase the value derived from evaluation and mutual recognition, improve certainty and consistency, facilitate international trade, enhance security assurance and create market access opportunities. Therefore, efforts to improve and augment the conformance-based assurance models should look first to the NIAP effort and related reform efforts.

V. Incentives

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.

Given the increased threat level of cyber attacks in the United States and around the world, and the need to keep this effort voluntary and industry-led, SIIA strongly supports the Green Paper's focus on offering incentives to organizations to develop improved cyber security plans, policies, procedures and operational cyber defenses.

SIIA also concurs with the Green Paper's suggestion that a meaningful national framework for data security and for breach notification should be enacted. Such a framework is necessary to prevent breaches and enhance consumer confidence, predictability and certainty for consumers, consumer protection authorities and businesses. To the extent that this initiative can lead to the improvement of security standards laid out in such a national framework, this could be a beneficial approach.

VI. Conclusion

Again, thank you for your thoughtful, timely proposal to craft a new framework to address internet security issues. SIIA appreciates the opportunity to comment, and we look forward to working with you on this very important issue. For further information or to discuss these comments, please contact Mark MacCarthy, VP, Public Policy at (202) 789-4471 or mmaccarthy@siia.net, or David LeDuc, Senior Director, Public Policy at (202) 789-4443 or dleduc@siia.net.