Before the
DEPARTMENT OF COMMERCE
Internet Policy Task Force

In the Matter of	)	
Cybersecurity, Innovation and the Internet Economy	)	Docket No. 100721305-0305-01

COMMENTS OF (ISC)2

Hord Tipton
Executive Director
33920 US Highway
Palm Harbor, FL 34684
(727) 683-0774

I am writing on behalf of (ISC)², a not-for-profit organization dedicated to improving the skills and capabilities of the global information security workforce through professional education and certification and public awareness. (ISC)² has certified over 70,000 information security professionals in 135 countries. We sincerely appreciate your continuing interest in the increasing security of the nation's broadband infrastructure and the promotion of vigilant cyber security public and communications providers.

We sincerely appreciate your continuing interest in the increasing security of the nation's infrastructure and the promotion of vigilant cyber security public and communications providers. We appreciate that the Department has creating its Internet Policy Task Force. A committed and focused effort by the Department with regard to the development of the digital economy is welcomed and appreciated. The Department can contribute to the multi-faceted effort to bolster our national cybersecurity posture.

We believe that through a well-crafted public-private partnership such a program can:

(1) Increase the security of the nation's infrastructure;

(2) Promote a culture of more vigilant cyber security among participants in the market for communications services; and

(3) Offer end users more complete information about their communication service providers' cyber security practices.

Quantifying the Economic Impact

The increased use and dependence on the Internet for commerce has led to an increase in the number of vulnerabilities to which we, as a nation, are exposed. As those vulnerabilities are exposed through system flaws or exploited by malicious actors, those compromises result in great financial loss, much of which is difficult to calculate. Through reports of system downtime, financial theft, incident response and mitigation efforts, internal misuse and loss of intellectual property, various reports on economic impact of those costs have been promulgated. Those calculations are developed normally from voluntary reporting so are incomplete estimates at best, and sorely understated at worst. Several studies do exist and provide information regarding financial losses from cyber incidents and should be included in reports. These studies include: the annual Computer Security Institute's survey, the RSA Online Fraud Report, the biannual Symantec Global Internet Threat Report, and the Verizon Business RISK Team Data Breach Investigations Report. While an accurate view of the actual and financial loss from cybercrime/cyber attacks would be useful, the information and thoughtful analysis we do have today in these reports should not be discounted.

All organizations have one common incentive to protect themselves: to retain the trust and confidence of their customer in order to remain viable in the marketplace. Additional incentives that would help provide for enterprises to share information regarding their breaches are: the existence of trusted custodians for information exchange between enterprises and, importantly, between industry and government that provides for privacy protection, protection of proprietary information, anonymity. Given the scope of the problems we face and the diversity of the community, we should consider that not just one entity or framework provides the answer for all, and a synergy among various entities could also be helpful. No matter what

mechanism(s) is used or created, it must accommodate the privacy of personally identifiable information, company proprietary information and copyright, and civil liberties concerns.

The loss of intellectual property and the downstream impact is a data set that is missing from reports listed above and one that is very difficult to determine. This is one area where more work could be done. Additionally, companies and groups are working to determine the opportunity costs associated with inadequate security. However, for many companies, particularly small and medium-sized businesses, the cost is too great for the investment for extensive preventive care. As such, we recommend that policymakers consider two possibilities to enable action: (1) developing a refundable tax credit for security measures, including adoption of best practices; and (2) ensuring that security measures are included in requirements for national programs (i.e. broadband and smart grid).

Raising Awareness

Regarding user education, there are many organizations, both public and private (corporations and not-for-profit organizations) that take on some level of effort regarding raising awareness for the end users. Each organization has their own mission and purpose, and each executes relevant programs to meet their targeted constituency. We are not aware of any analysis that has been done to categorize these efforts and provide a group of best practices and return on investment outside of the education community.

More to the point, we support user education and awareness efforts, both in the classroom and out. We support a concerted, nationwide, public service campaign such as that as is being undertaken by the National Cyber Security Alliance (NCSA) and (ISC)², which also sponsors staysafeonline.org. More funding and a focus on partnership could significantly bolster NCSA's

good work to date. It is important to note that many companies engage in a variety of user awareness activities in their communities, in their cadre of employees, and in their customer base.

At the university levels, we also have an opportunity to engage our students not only in ways they can protect themselves online but also to engage them in activities that can lead to their cultivation as the very engineers, programmers, and other technologists that will continue and enhance innovation in technology and security. While there is a smattering of creative training activities across the country, concerted training efforts such as cyber challenge competitions, apprentice programs, and internships can be bolstered with greater senior level commitment and funding.

With regard to raising awareness in the industry about the resources available to them, the key words are: public-private-partnership. In both strategic risk management for critical infrastructure protection and in operational information sharing and analysis efforts, there is a robust program for engagement by virtually every enterprise in the country. With regard to resources, more can be done to inform the government and business community about ways they can get more information about technology trends, risk management and mitigation efforts, technical assistance, partnership opportunities, and other benefits. It is important to note, however, that some of these services exist in the marketplace today, and direct duplication would hamper competition and competitiveness and in the worst case, diminish security.

Finally, a key component of raising awareness for enterprise users is to know what threats they are facing. We have long been challenged by the inability to share useful and actionable threat information between industry and government, but we need to find a way to do it.

Web Site and Component Security

The notice of inquiry poses the question whether the government alone, the private sector, or the government and the private sector collaboratively explore whether third-party verification of web site and component security is, or can prove effective in reducing the proliferation of malware. We regard that this kind of analysis – and innovation – is already underway in the private sector and may not need government intervention. If government is involved, it should be in partnership in order to address cost, collaboration, and cooperation in the environment. Additional questions would include what standards to use, depending on risk; how to identify all web sites and their components (who would do that, and who would evaluate the results); and who would determine what needs to be fixed and in what order. In addition to addressing these governance challenges by enterprises, operationally the process would need to be recurring and repeatable to reflect the ever-changing technology and threat environment.

Authentication/Identity (ID) Management

In regards to improved authentication/Identity Management, we believe that sufficient technology is available to meet the future needs of improving the current need; however, business and government need to allocate resources to meet the needs of improving upon the current environment. Government action on the implementation of HSPD-12 will, in the long run, pay dividends in strengthening both authentication and identity management. A similar program for the business environment is necessary and might be best accomplished by the states in the development of a secure identify card and have the government provide funds and

incentives to enterprises. On infrastructure, again, the government should provide support and tax incentives, to encourage the development of a safer infrastructure since most is in private hands. The government should consider a coordinated education campaign to inform the public of the benefits of building a stronger infrastructure and the need of stronger authentication and identity management for continuing development of global commerce. Since authentication and identity management methods will require additional features beyond the current password regime, the government is ideally suited to provide the messaging, fund the improvements and influence the private sector in adapting to the changes necessary. Government should manage outreach to economies, industry, and consumers regarding cybersecurity and cyber ethics that emphasizes (1) safety and security best practices; (2) the benefits and responsibilities of using information networks; and (3) the potential negative consequences resulting from the misuse of networks.

Global Engagement

Cyberspace is borderless, so we encounter global considerations regarding cybersecurity every single day. On the one hand, we cannot stop attacks at our traditional borders, so we need to be engaging with international partners on a sustained basis to leverage partnerships, information, and capabilities to greatest extent possible. On the other hand, our multinational companies, small, medium, and large, are engaging in global commerce and have customers, suppliers, and employees all over the world. As they engage in business in other countries, they encounter challenges to both business operations and cybersecurity efforts.

First, there is a wide range of levels of understanding about the importance of cybersecurity in other countries, customers, and end-users. All present problems for business facilitation and security. As such, there are greatly varying levels of resource in other countries

to go to for help for information gathering for greater situational awareness, incident response collaboration, or law enforcement cooperation. In all cases, our companies are hampered by lack of knowledge or coordination points for the quickest possible and appropriate action. Therefore, it is crucial for the U.S. Government to take a leadership role in the global community on cybersecurity to forge important linkages and help build capacity. TechAmerica has long supported the creation of a position of Ambassador for Cybersecurity at the Department of State to coordinate international engagement and strategy. In addition, the U.S. Government's diplomatic efforts in this regard would be well-served by the establishment of a cadre of dedicated "cybersecurity attaches" in U.S. embassies around the world.

Second, our multinational companies often encounter cybersecurity measures by other governments as a market entry or business barrier in the host country. Some countries have tried to demand source code or encryption keys from U.S. companies under the auspices of cybersecurity. In other instances, countries try (and in some cases succeed) to put in place requirements for U.S. companies to operate in the domestic market such as: partnership or technology transfer requirements; legal liability requirements for corporate officers; privacy protection requirements that hamper needed security measures; prohibitions on transborder data flows;

Third, with regard to standards, the best way for the U.S. Government to better encourage the use of internationally accepted cybersecurity standards and practices outside of the U.S. is to not create its own standards and global supply chain rules that directly contradict them or indirectly confuse implementation of two sets of standards.

As a final note, the U.S. Government should continue its participation in existing multilateral, regional, and bilateral forums in which cybersecurity is a subject for dialogue,

negotiation, or development. To the greatest extent possible, the U.S. Government should be sure to engage the private sector in the development of policy positions and capacity building/partnership programs in those forums and bilateral relationships in order to develop and cultivate norms for behavior that support greater global cybersecurity. Utilizing existing – and, therefore, established – forums will be more beneficial than trying to create a new body that will have to consider all manner of governance and diplomatic protocols before even beginning to make progress. In addition, utilizing non-negotiating forums such as the Internet Governance Forum, the Forum for Incident Response and Security Teams (FIRST), and other arenas for dialogue would supplement more formal interactions with established partnerships such as those being driven through the Department of Homeland Security's National Cyber Security Division for government-to-government collaboration and cooperation.

Product Assurance

(ISC)² supports the concept of third party validation mechanisms that are licensed and trustworthy. International Standards Organization (ISO) 15408, the International Common Criteria, is the international standard for security assurance and has a robust construct of evaluation labs that are licensed and certified to conduct product reviews.

We recognize that standards and corresponding certifications are only as good as both the input and the application of the standard or certification. In the case of the Common Criteria, improvements to streamline the evaluation process are essential to meet the business environment otherwise the evaluation process is too unwieldy and not cost effective. Fortunately, many of those improvements are currently underway. However, even a perfect standard and certification will be ineffective if not properly utilized by its customer base.

Government can work to close gaps and exceptions in procurement processes that allow acquisition officials to ignore certification and standards for security assurance.

We understand that while certifying products is a benefit, the process is often too heavy handed and needs to be more agile so that the process is able to meet different levels of need or risk. We believe that such a discipline can be found in the principle of accountability. Policies that include processes for securely developing products should include the existence of secure processes for the product development lifecycle (e.g., sound requirements and specifications, coding, review, testing and validation) and evidence that security training and education programs are available and mandatory for engineers and developers as well a broader set of employees that impact product development. Progress in building these accountability criteria and requirements are a useful path to effective Common Criteria modification and implementation. The goal should be to drive a global criterion and requirements, as divergent national standards run the risk of creating significant market entry barriers for new technology, and undue compliance complexity for technology slows product introduction that is intended to be sold worldwide.

Research and Development

(ISC)² is a supporter of increased funding for cybersecurity research and development and advocates for a coordinated, public-private approach to determining priorities and implementing research and development programs. Government should provide incentives for long-term projects by providing for tax incentives for private R&D efforts or through direct funding of R&D in academic institutions. In all cases, coordination and collaboration is key to ensuring that gaps are identified and priorities set to avoiding duplicative efforts.

Regarding a federal government-sponsored “grand challenge program” to draw attention to and promote work on specific technology problems, we believe the verdict on its effectiveness may be mixed. We would suggest that such an effort could be effective IF government and industry collaborate on the development of a concept/program design; if multiple channels for communicating and marketing the program were utilized in a cohesive manner by both government and industry; and if federal funding were attached to the program in some way.