USCIB

UNITED STATES COUNCIL FOR INTERNATIONAL BUSINESS

September 22, 2010

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899

Re: USCIB Comments on Cybersecurity, Innovation and the Internet Economy

Dear Ms. Honeycutt:

We are pleased to provide comments in response to the Notice of Inquiry. Given our specific mandate and expertise, we have focused our remarks on the portions of the NOI pertaining to raising awareness, global engagement and establishing an incentives framework.

The United States Council for International Business (USCIB) promotes open markets, competitiveness and innovation, sustainable development and corporate responsibility, supported by international engagement and prudent regulation. Its members include top U.S.-based global companies and professional services firms from every sector of our economy, with operations in every region of the world. With a unique global network encompassing the International Chamber of Commerce, the International Organization of Employers and the Business and Industry Advisory Committee to the OECD, USCIB provides business views to policy makers and regulatory authorities worldwide, and works to facilitate international trade and investment.

USCIB's ICT Policy Committee represents businesses from diverse industry sectors. The committee advocates for sound international policy frameworks, characterized by free and fair competition, minimal government intervention, free information flows and a user orientation, that ensure the continued growth of ICTs and extend their benefits around the world. The committee also increases awareness of the potential impact of policies, laws, and regulations related to ICTs and e-business. We promote self-regulation and the application of existing global guidelines to ensure responsible and accountable implementation of new technologies and applications such as radio-frequency identification (RFID) and social networking. We promote a global culture of cyber-security through ICC and BIAC, and in regional fora.

We are pleased to see the results of initial industry listening sessions reflected in the NOI itself. Indeed, we believe there are distinct roles for different stakeholders and organizations, some of which are outlined below. The NOI recognizes the significant economic impact of cybercrime and the effort industry has taken to combat cybercrime and to continually keep pace with rapidly evolving cybersecurity risks. We encourage the Department of Commerce to continue to prioritize ensuring that the Internet remains an open and trusted infrastructure for all users and welcome this opportunity to identify leading policy challenges and to recommend possible solutions.

Raising awareness

Cybersecurity is often thought of in the context of technology – how to secure systems from threats -but must also be considered in terms of behavior and understanding. When the OECD was reviewing its security guidelines many people referred to a "culture of security" to denote the need to make sure that this was not just a consideration for security experts, but for all corporate employees as well as users of systems of all kinds. One of the main principles of those security guidelines was for everyone to take responsibility appropriate to their role. Thus individuals may need to update virus programs and participate in automated patch management programs for installed software. They should be careful with their password and who is granted access to their systems either directly or via downloaded applications. Finally individuals might need to be aware of the types of the threats they may face from phishing to identity theft to cyberstalking and cyberbullying. Obviously greater responsibilities were placed on corporations and other more formal institutions, but it is important to focus on individual responsibilities because it is not clear that with ever more complex systems, individuals can indentify threats or appropriate steps to take to mitigate risk.

While technology is getting more accessible and perhaps intuitive in use, the complex systems and interactions that support such uses are being obfuscated by the very usability. The need to hide the complexity for ease of use may be contributing to further information asymmetry in terms of risks and methods of protection. The ability to create professional looking websites, or spoofs of websites with little expertise and inexpensive tools creates the potential for fraud and confusion. The multiple vectors through which malware and viruses may spread create issues with botnets and corruption of individual systems.

Outreach and awareness-raising across all stakeholder communities is needed to alert users of systems to possible dangers and to promote good practices that help make users less susceptible to threats. Part of this issue is being addressed by industry that is developing more user-friendly ways or patching or updating virus protection and screening tools for malware. Despite many one touch solutions, surveys still find significant number so systems with virus protections installed have out of date definitions which impair their ability to protect systems. This is where awareness raising must go towards a cultural or behavioral solution. Look both ways before crossing the street, test a drink for temperature before taking a big sip, wash your hands before eating are just some of the behaviors we are accustomed to. They are taught at home, by experience and reinforced in schools. We must undertake similar efforts for cybersecurity or the basics of good security hygiene.

In the case of cybersecurity, the home may be the most problematic space for teaching lessons as the children are often more skilled than the parents. This may present a win-win opportunity allowing children to work with parents in assuring the security of home systems. There are some limits to the benefits here as children may be better placed to undermine certain content filters and parental oversight mechanisms. Interestingly there has been some indication that this is a place where technology helps bridge generations. Many grandparents have discovered technology provides connections with distant grandchildren which could provide another potential for awareness-raising in both directions across generations.

Today, a number of programs exist in schools, through corporate foundations and not for profit groups to expose children across all age groups to concepts of security, netiquette and responsible online behavior. Programs include concepts of using students as mentors in participating schools (TeenAngels), programs to provide secure online learning environments as well as help training teachers in the use of technology to educate (ThinkQuest). These programs need to be supported and expanded, both domestically and internationally. Cybersecurity threats know no national boundaries and the cultural and behavioral responses need to be equally global. Cybersecurity education and awareness is not limited to younger children in schools. As students gain experience and greater access to technology it becomes more ingrained in all aspects of their life. Education and awareness-raising are thus needed through education, work life and into retirement. Technologies continue to evolve as do threats and solutions – there is no point in time when this process is complete.

Many efforts are underway by government, the private sector and academia. This space may benefit most from public private partnerships as some best practices suggested by companies may include the need to update software or undergo training which users might confuse with marketing or an up sell. Public-private messaging on the importance of security and the need to address appropriate responsibilities by individuals, SMEs, enterprises , organizations and governments is needed to assure better uptake of existing solutions.

In considering cybersecurity, we have discussed education as a way of instilling responsible behaviors that may limit exposure to threats. Greater focus on comprehensive security curricula in schools that teach ICT skills would also help improve the state of the art and skill sets of students being hired by industry to develop or implement technology solutions. While many companies have developed secure coding and development practices, they need to be properly executed by people who are well grounded in security basics. More collaborative work among the private sector, government and academia in developing and funding this security coursework needs to be explored. There have even been suggestions that such skill sets could be evaluated or certified in an appropriate manner to allow companies to have greater confidence that all candidates with such evaluations would have a generally accepted security skill set.

One last role for education is linked to workforce training. A number of companies have introduced awareness training for security, privacy, ethics and other relevant topics. The cost and time involved, however makes this more relevant to larger companies. Attention needs to be paid to how to assure that SMEs have such resources available. It is unlikely that they have the time, expertise, or resources to develop customized training, so they will need to turn to trade associations, government entities or academic institutions to help provide such training. It would be useful for the government to fund research into what type of training is most effective and to work with relevant stakeholders in its development and deployment. One last consideration in workforce training would be the ability to raise security awareness among displaced workers that might be transitioning from more manual or administrative tasks to tasks with greater ICT use. Laid off workers could be given basic courses in ICT skills and security awareness as part of transition/reintroduction to the workforce program. Such programs could be offered at local schools or universities through some form of public private partnership.

Global engagement
New innovations in ICT come about every day, from all corners of the globe, and continue to drive the GDI into the future. Yet, this process is stalled and sometimes blocked by a confusing and often conflicting array of country specific laws and regulations. Because of concerns about security, the need to develop policies aimed at making the digital environment reliable and secure is becoming an important agenda item for governments and policymakers around the world. However, a siloed, country-specific regulatory approach may unintentionally disrupt a networked environment dependent upon global interoperability and connectivity without providing any incremental security benefit.

We can look both to past efforts such as the key escrow scheme considered by the U.S. in the 1990s and ongoing regulatory efforts in the encryption area in a number of jurisdictions to provide further support for this concept. Currently, encryption laws and regulations in the U.S., China, Russia and other countries variously impose regulations ranging from limited export controls to import authorization/declaration requirements for ICT products with cryptographic technology to restrictions on distribution, sales and use of such products (including R&D and manufacturing in some cases).[1] Some of these regulations have the impact of requiring the adoption of certain country specific standards and technologies, which run the risk of mandating a particular technology as the innovation that must be deployed. Even the application of more limited encryption export controls by the US is increasingly creating burdens and supply chain instabilities, since the substantial liberalization of the controls a decade ago are now being outpaced by the pervasiveness of encryption capability in ICT products.

Navigating the increasingly confusing and non-harmonized patchwork of global requirements with respect security to extract elements common across cultures presents challenges. We are particularly concerned about the following being taken by some governments:

- **Mandatory source code escrow or disclosure** and other sensitive design elements are unprecedented and unacceptable to the global ICT industry. This is sensitive proprietary information at the core of a company’s business. Even if this were acceptable to vendors, as in some cases key design components may be licensed from third parties, it would complicate a vendor’s ability to comply with this requirement. In any case, this requirement is unprecedented and seemingly unrelated to security.
- **Transfer of technology provisions**
- **Mandatory contracts** between two private parties.

We offer a few recent examples:

- **India encryption regulations -** In December 2008, the Government of India (GOI) amended the Information Technology Act 2000 and passed the Information Technology (Amendment) Act 2008 which included broader power for the government to regulate IT for security and privacy. Section 84A of this amended act allowed for new encryption regulations to be implemented in light of complications the government has experienced

[1] See, e.g., Regulations on the Administration of Commercial Cipher Codes, promulgated and effective as of October 7, 1999, Provisions on the Administration of Production of Commercial Cipher Products, promulgated, and effective as of January 1, 2006, and Provisions on the Administration of Commercial Cipher Research, promulgated, and effective as of January 1, 2006.

in intercepting communications, including while it was responding and investigating the bombings in Mumbai in November of 2008.

- **India telecommunications security requirements -** On May 18, 2010, the GOI issued a new regulation, document 10-15/2009-AS.III/193 detailing security clearance requirements, for telecommunications equipment being procured by service providers operating in India. The regulation specified that service providers much apply for security clearance of equipment/software as prescribed by document 10-15/2009-AS.III/139, issued in February 2010. The May regulation further stated that passive equipment and locally manufactured equipment would not be subject to the regulations. It further stated that the clearance is required for core equipment and not components.

  On July 28th 2010, the Department of Telecom issued order No. 10-15/2009-AS.III/Vol.II/(Pt.)/(25) amending the Unified Access Service License Agreement for security related concerns for expansion of Telecom Services in various zones of the country. This order mandated a template be signed by the vendors and the operators for the procurement of equipment which included a clause for escrowing of source code and transfer of technology.

- **China Compulsory Certification (CCC)**—in August 2007, the China National Certification and Accreditation Administration (CNCA) announced mandatory testing and certification for 13 categories of security enhanced technology hardware and software. The CCC is based on Chinese security standards, not on international standards such as ISO or the Common Criteria. In March 2008, the CNCA announced which specific products in these 13 categories would be required to obtain the CCC mark. In April 2009, China decided to require compliance "only" for government procurement, rather than for commercial sales to "strategic sectors." The U.S. government and industry have argued that China should withdraw the CCC scheme, and instead use international security assurance standards.

- **Multi-Level Protection Scheme (MLPS)**— In 2007, the Chinese government announced MLPS, which applies mandatory security requirements to the development, deployment, management and use of information technology. It applies to a broad spectrum of sectors, including finance, transportation, energy, telecom and Internet, etc. While it is originally based on the "Orange Book" – a 1980's standard for the assessment of computer security controls that has been replaced by the more modern Common Criteria – MLPS includes additional requirements that are specific to China and at variance with international standards and requirements. Among the most problematic requirements of the MLPS, for products rated at level 3 and above, are: the developer and manufacturer must be Chinese companies owned by Chinese citizens; the core technology and key components of products must be based on Chinese intellectual property rights; and any product incorporating cryptographic functionality must receive approval from the Office of Security Commercial Code Administration (OSCCA), and cannot be an imported product, except with approval of the State Encryption Management Bureau (SEMB). The SEMB enforces the implementation of Chinese cryptographic algorithms, and imposes import and export licenses and requires the escrow of source code for software implementing cryptographic functionality.

- **Trusted Cryptography Modules**—China has opted against allowing the use of Trusted Platform Modules (TPMs) – chips that perform specific security tasks, such as verifying that only authorized code runs on a system – which comply with the internationally-accepted standard recognized by the International Organization for Standardization (ISO.) Instead, China is developing its own standards that will build upon, and enforce the use of, Chinese cryptographic algorithms (see above reference to SEMB).

The USG has an important role in ensuring that the development of policy and legal infrastructure globally promotes continued innovation and enabled economic growth. In developing solutions to the security challenges in the online environment, the USG should look to global standards and avoid creating geographically siloed regulations that may impede the global interoperability and network connectivity that have spurred the growth of the GDI. This is perhaps the best way the USG can encourage the use of global standards and best practices outside the U.S. It is also important that the USG avoid taking confrontational action which may provoke an equal or even more severe reaction in the form of country specific regulation in other geographies.

Incentive Frameworks

Improving cyber security across the wide array of stakeholders that build, participate in, and rely upon access to the national, interconnected networks is a challenge – due in part due to the diversity of the owners, operators and end users of interconnected networks – private sector (small, medium, and large enterprises), individuals citizens/consumers, governments. However, these entities must all make decisions that affect the "security" of cyberspace – making decisions about resources, processes and technologies to protect their "assets". Their choices can, and often are, influenced by a cost benefit analysis – an analysis as to whether the risk is sufficient to merit the investment or reallocation of limited resources (human or financial). Regardless of particular regulatory mandates that may or may not apply in individual economic sectors, there may be compelling business models for some to mitigate cyber risk through investment, while others are unable to make that case.

Promotion of incentives for investment in and deployment of cyber security solutions would significantly enhance the overall security of our national infrastructure. The Department of Commerce can and should play a role in identifying and recommending such incentives, and when accompanied by increased educational efforts and global engagement, these incentives will help make a more compelling business case for adoption of both cyber best practices and technology solutions across the full range of stakeholders.

We recommend that the Department explore the following incentives options, which together or taken individually, offer opportunities for this Administration to enhance the cybersecurity posture of our country.

- Promote the use of federal and state procurements to require cyber security capabilities – whether through cyber certifications or other methods. However, any requirements should be for the outcome, not the specific technologies, to ensure the flexibility to respond the constantly evolving nature of cyber threats.

- Promote R&D funding of cybersecurity solutions – both technologies and processes.
- Promote tax incentives for investment in cybersecurity – examples could include tax rebates both for individual and corporate investment in continual upgrades in cyber solutions and tax deductions or credits for investment in cybersecurity training,
- Expand existing liability protection schemes to cyber-certified solutions. For example, in collaboration with the Department of Homeland Security, clarify the scope of the existing SAFETY Act to cyber solutions. Otherwise, promote the creation of a new Cyber SAFETY Act.

We thank you for this opportunity to comment and look forward to continued discussions with the Internet Policy Task Force on these important issues and on any recommendations that result.

Sincerely,

Peter M. Robinson