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

September 20, 2010

Ann Beauchesne
Vice President
National Security & Emergency Preparedness Department

Via e-mail: cybertaskforce@doc.gov

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

Dear Ms. Honeycutt:

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, writes to thank the Department of Commerce for collecting public comments on its Notice of Interest (NOI) entitled "Cybersecurity, Innovation, and the Internet Economy."[1] The NOI covers a wide range of promising topics for discussion and debate as well as a lengthy list of questions. The Chamber has not attempted to answer every question. Instead, we have focused on issues that are priorities of ours and may be helpful to department leadership in its review of cybersecurity challenges in the private sector.

Quantifying the Economic Impact

Research suggests that cybercrime in the United States is on the rise. While it is challenging to get a complete picture of the problem, organizations such as the Internet Crime Complaint Center (IC3), a joint operation between the FBI and the National White Collar Crime Center, provides a window into a growing trend. According to IC3's *2009 Internet Crime Report*, annual crime complaints reported to IC3 have increased 668% when compared with data from the 2001 annual report. Complaint submissions for 2009 were 336,655, a 22% increase from 275,284 in 2008 and a 63% increase from 206,884 complaints in 2007. This complaint total includes many different types of crimes, including both fraudulent and nonfraudulent crimes. The dollar loss from all cases of crime referred to law enforcement totaled $559.7 million, a 112% increase from $264.6 million in 2008.[2]

[1] See 75 Federal Register, pp. 44216-44223, http://edocket.access.gpo.gov/2010/pdf/2010-18507.pdf; http://edocket.access.gpo.gov/2010/pdf/2010-22774.pdf (docket numbers 100721305-0305-01, July28, 2010; 100721305-0436-02, Sept. 14, 2010).

[2] Internet Crime Complaint Center (IC3), *2009 Internet Crime Report*; see Mar. 12, 2010, IC3 press release and report, respectively, at www.ic3.gov/media/2010/100312.aspx; www.ic3.gov/media/annualreport/2009_IC3Report.pdf.

However, IC3 research indicates that only one in seven incidents of fraud ever makes its way to the attention of enforcement or regulatory agencies. Similarly, the Bureau of Justice Statistics' National Computer Security Survey finds that most cyberattacks against businesses go unreported to law enforcement authorities.[3]

The Department of Commerce's NOI asks if there are adequate incentives for businesses to provide information about successful computer intrusions (hacking) or security breaches. Federal laws such as the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act require institutions to meet various standards for safeguarding customer and patient records. Also, as concerns over identity theft and data security have increased, at least 46 states have enacted legislation requiring notification of security breaches involving personal information.[4]

The Chamber believes that there are too few positive incents for companies to reveal information about security breaches. The costs of public disclosure remain high and might take several forms, including: financial market impacts, reputation effects, and litigation and liability concerns.[5] Policymakers can play a role in providing clearer statutory protection for information shared with government by business. For instance, public policy should reflect that any information shared by companies related to cybersecurity have liability protection from Freedom of Information Act disclosure and use in a civil trial.

Raising Awareness

Several U.S. presidents have declared the protection of our nation's digital infrastructure to be a top economic and national security issue. While extensive public and private sector efforts have been ongoing for years, President Obama articulated in May 2009 the need for wider public participation in protecting America's cyberspace. He called for a national public awareness and education initiative to promote cybersecurity, which the Chamber strongly supports.

The NOI asks about the efficacy of education efforts and the adequacy of information sharing and incident reporting programs. Public and private sector stakeholders in the area of cybersecurity can readily point to awareness and education programs that draw upon industry best practices. For instance, the National Institute of Standards and Technology, the Small Business Administration, and the FBI have conducted a series of training meetings on computer

[3] U.S. Department of Justice, Bureau of Justice Statistics, *Cybercrime against Business, 2005*, Sept. 17, 2008, http://bjs.ojp.usdoj.gov/index.cfm?ty=pbdetail&iid=769, p. 7.

[4] National Conference of State Legislatures; see list of security breach laws at www.ncsl.org/Default.aspx?TabId=13481.

[5] See Brian Cashell, et al. *The Economic Impact of Cyber-Attacks*, Congressional Research Service (CRS) report (RL32331), Apr. 1, 2004, p. 13.

security for small businesses.[6] There are many more worth mentioning. Still, cybersecurity education is relatively new and uncoordinated nationally.

The NOI suggests organizations that have experienced cyber intrusions or attacks do not know with whom to share that information or how to seek assistance. Based on anecdotal evidence, this perception seems to be accurate. Recognizing this hurdle, the Chamber's forthcoming cybersecurity guide for businesses purposefully lists several organizations—e.g., OnGuard Online (www.onguardonline.gov), IC3 (www.onguardonline.gov), and United States Computer Emergency Readiness Team (www.us-cert.gov)—to help businesses file complaints on matters such as hacking, economic espionage, online extortion, international money laundering, identity theft, and a growing list of Internet-facilitated crimes.

The NOI asks also if the U.S. government is adequately resourced to assist businesses during or after a cyber incident. Several terrific public-leaning entities, such as ones noted above, have been created to assist private sector entities, but they are likely not well known to most business people. Government and private sector stakeholders need to continue to publicly promote organizations such as OnGuard Online and US-CERT and encourage businesses to engage them. Also, consideration should be given to the establishment of a cybersecurity service center to assist the business community in implementing protection measures, sharing information about cyber threats reported by businesses, and dealing with cybersecurity incidents that occur. Few government entities, whether at the federal, state, or local level, are adequately resourced to serve as a "911" responders to assist most businesses with handling cyber incidents. As cyber threats grow in scope and sophistication, there is a need to enhance partnerships at all levels of government to assist private sector entities that have become victims of a broad and expanding variety of cybercrime.

In 2008 and 2009, the Chamber partnered with the Department of Homeland Security's National Cyber Security Division to increase businesses' awareness of cybersecurity from an enterprise risk management perspective. With roughly 85% of the nation's information and communications infrastructure in private sector hands, cybersecurity awareness and education needs to be given greater public-private attention than it receives. The Chamber-DHS campaign revealed that there is considerable public hunger for outreach and education initiatives.

The NOI asks about the adequacy of information sharing and situational awareness programs. The Chamber seeks to frame "information sharing" in the context of expected outcomes, such as spurring the sharing of specific and actionable intelligence between the government and the private sector to mitigate risks and imminent threats. A key goal is enhancing operational capabilities for greater situational awareness (e.g., "What are the threats on my network?") to defend against cyberattacks on corporate networks and the cyber commons (a vulnerability in one system may represent a vulnerability to others). Too often, industry representatives report that information is shared with government agencies, but little if any

[6] See National Institute of Standards and Technology, Computer Security Division, "Small Business Corner," http://csrc.nist.gov/groups/SMA/sbc/index.html.

information of value is received in return.[7] An informed defense against a cyberattack is a key component of effective deterrence.

Global Engagement

The Chamber supports U.S. engagement in multilateral forums that promote a global approach to address cybersecurity standards and prosecute cybercrime, such as the Council of Europe Convention on Cybercrime. The Chamber is encouraged that a group of 15 nations—including the United States, China, and Russia—have recently endorsed recommendations to the United Nations to reduce threat of attacks on computer networks of member nations. [8] We support the administration's diplomatic efforts to create internationally accepted "cybersecurity principles," exchange information on national legislation and cybersecurity strategies, and strengthen the capacity of less-developed countries to protect their computer systems. Significantly, as the NOI highlights, policymakers must avoid the "balkanization of the global marketplace due to a proliferation of mandated, sometimes unique cybersecurity standards and conformity assessment requirements among nations—leading to a diverse patchwork of national requirements that can inhibit trade."

Product Assurance

The Chamber recognizes the importance of securing global and national supply chains. Important elements of the government, including U.S. military and intelligence communities, and the private sector increasingly depend on dynamic information systems as part of our global economy. The disruption of high volume transaction systems or supply chain operations could have serious implications for national and economic security. Government and industry have a mutual interest in promoting a risk-based strategy to secure their information systems from development to acquisition and through their operational life cycle.

The Chamber promotes procurement approaches that leverage industry competition and best practices. The December 2008 Center for Strategic and International Studies (CSIS) cybersecurity report notes that cooperation with the private sector regarding federal procurement reform will be essential for success. Procurement reform could take the form of the government defining performance requirements for the products and services it acquires rather than setting design specifications that would regulate how software is written or hardware is manufactured.

Research and Development

The Chamber supports the federal Networking and Information Technology Research and Development, or NITRD, Program that has identified three initial R&D themes: to direct attention to investigations that change the game to enable risk-aware safe operations in compromised environments, to increase adversaries' costs and exposure and support informed trust decisions, and to allow for effective risk/benefit analyses and implementations. The

[7] A case in point: At an Oct. 27, 2009, House Energy and Commerce Committee hearing on cybersecurity legislation, representatives of the electric power industry and government energy regulators noted that, beyond known vulnerabilities, specific actionable information has not been provided to the private sector by federal authorities regarding digital threats to their systems.

[8] Ellen Nakashima, "15 nations agree to start working together to reduce cyberwarfare threat," *Washington Post*, July 17, 2010, www.washingtonpost.com/wp-dyn/content/article/2010/07/16/AR2010071605882_pf.html.

Chamber is particularly interested in research topic entitled Cyber Economic Incentives.[9] Technology alone cannot defeat cyber threats. Secure practices need to be understood and incentivized if cybersecurity is to become as ubiquitous as the PCs and handheld devices that we rely on so intensely in our daily lives.

For business owners and managers facing cyber risk, the "bottom line" question is how much to spend on information security. There may never be a one-size-fits-all approach, but ideally the research will provide organizations, including small businesses, with what may constitute an optimal amount of security spending—spending that's neither too high nor too low.[10]

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."[11]

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 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.

Conclusion: Policymakers Should Reinforce Public-Private Collaboration

Despite the fact that more than 85% of critical infrastructure in the United States is owned and operated by the private sector, cyber response capabilities are not always well coordinated due to inadequate collaboration and information sharing between and among the

[9] See Networking and Information Technology Research and Development Program, "Federal Cybersecurity Game-change R&D," http://cybersecurity.nitrd.gov.

[10] See previously cited CRS report, pp. 17, 21.

[11] James A. Lewis et al. 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.

public and private sectors. Public-private partnerships are vital because the “response baton” may need to be passed quickly from industry to the public sector (e.g., law enforcement). Either the nature of a cyberattack outstrips a company’s ability to respond effectively or it may be difficult to determine whether the attacker is an individual hacker, an insider threat, or a nation-state actor. The Chamber urges policymakers to focus on improving coordination and bridging the preparedness and response gaps that exist among businesses and federal, state, and local responders. Policymakers should advance positive incentives to shape public behavior and improve cybersecurity.

The Chamber welcomes the Department of Commerce’s review of the connections between cybersecurity challenge in the commercial sector and innovation in the Internet economy, and we look forward working with the department, other agencies, and Congress on these important issues. Thank you.

Sincerely,

Ann Beauchesne

Ann Beauchesne
Vice President