100 Years Standing Up for American Enterprise

U.S. CHAMBER OF COMMERCE

Statement of the U.S. Chamber of Commerce

ON: **Securing America’s Future: The Cybersecurity Act of 2012**

TO: **U.S. Senate Committee on Homeland Security and Governmental Affairs Committee**

DATE: **February 16, 2012**

The Chamber’s mission is to advance human progress through an economic,
political, and social system based on individual freedom,
incentive, initiative, opportunity, and responsibility.

The U.S. Chamber of Commerce is the world's largest business federation representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

More than 96% of the Chamber's members are small businesses with 100 or fewer employees, 70% of which have 10 or fewer employees. Yet virtually all of the nation's largest companies are also active members. We are particularly cognizant of the problems of smaller businesses, as well as issues facing the business community at large.

Besides representing a cross section of the American business community in terms of number of employees, the Chamber represents a wide management spectrum by type of business and location. Each major classification of American business—manufacturing, retailing, services, construction, wholesaling, and finance—is represented. Also, the Chamber has substantial membership in all 50 states.

The Chamber's international reach is substantial as well. It believes that global interdependence provides an opportunity, not a threat. In addition to the U.S. Chamber's 115 American Chambers of Commerce abroad, an increasing number of members are engaged in the export and import of both goods and services and have ongoing investment activities. The Chamber favors strengthened international competitiveness and opposes artificial U.S. and foreign barriers to international business.

Positions on national issues are developed by a cross section of Chamber members serving on committees, subcommittees, and task forces. More than 1,000 businesspeople participate in this process.

The Honorable Tom Ridge
Chairman, National Security Task Force, U.S. Chamber of Commerce
U.S. Senate Committee on Homeland Security and Governmental Affairs Committee
Hearing Entitled, "Securing America's Future: The Cybersecurity Act of 2012"
Thursday, February 16, 2012

Good afternoon, Chairman Lieberman, Ranking Member Collins, and other distinguished members of the Homeland Security and Governmental Affairs Committee.

I am Tom Ridge, President and CEO of Ridge Global. Prior to heading Ridge Global, and following the tragic events of September 11th, I became the first Assistant to the President for Homeland Security. In 2003, I was honored to become the first Secretary of the Department of Homeland Security (DHS).

During my tenure, I had the privilege to work with more than 180,000-plus employees from a combined 22 agencies to create an agency that facilitated the flow of people and goods; instituted layered security at air, land, and seaports; developed a unified national response and recovery plan; protected critical infrastructure; integrated new technology; and improved information-sharing worldwide. Before September 11th, I was twice elected Governor of Pennsylvania and served from 1995 to 2001. Prior to being governor, I proudly served in the House of Representatives, beginning in 1982.

I am testifying today on behalf of the U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than 3 million businesses and organizations of every size, sector, and region.

I chair the Chamber's National Security Task Force, which is responsible for the development and implementation of the Chamber's homeland and national security policies. It is composed of 150 Chamber members who represent a broad spectrum of the nation's economy. The Task Force seeks to identify current and emerging issues, craft policies and positions on issues, and provide issue analysis and direct advocacy to government and business leaders.

On behalf of the Chamber and its members, thank you for the opportunity to appear here regarding cybersecurity and ways in which we can secure America's future. I have valued the discussions that we have had on policy when I was in the public sector.

Introduction: Cyberspace Offers Tremendous Opportunities and Challenges

The business community recognizes the opportunities and challenges inherent in our interconnected world. The Internet has transformed the global economy and connected people in new and exciting ways. It helps drive progress in almost every aspect of our lives. Businesses of all sizes are increasingly dependent on the Internet for their day-to-day operations. Cyber technologies help businesses achieve great efficiencies, and they help run our vital infrastructures—from the shop floor to energy production to banking and much more.

Unfortunately, bad actors—such as organized criminals, “hactivists,” and foreign governments—have taken advantage of a cyber environment that is more open and welcoming than secure. The Chamber and members of its National Security Task Force are keenly aware of cyber threats to American businesses and the nation. The Director of National Intelligence, James Clapper, recently testified about the scope and nature of cybersecurity incidents as well as the range of actors and targets. His insights help inform our discussion.

An essential question facing policymakers is: How do we continue to develop public policies that improve economic and national security? The Chamber believes there is a growing consensus about measures that can help counter illicit cyber intruders and earn broad bipartisan support, which I will touch on further in my remarks. Over the past few years, the Chamber has stated that it will support legislation, such as an information-sharing bill, that is carefully targeted toward effectively addressing the complex cyber threats that businesses are experiencing.

The Private Sector Strives to Proactively Enhance Its Security and Resilience

Businesses strive to stay a step ahead of cybercriminals and protect potentially sensitive consumer and business information by employing sound risk-management principles. Industry has been taking robust and proactive steps for many years to protect and make their information networks more resilient.

The protection of U.S. critical infrastructure has a lengthy history. Issued in 1998, Presidential Decision Directive No. 63 (PDD-63) helped spur the protection of critical infrastructure and cybersecurity and as well helped launch the formation of Information Sharing and Analysis Centers (ISACs) across the private sector. In 2003, Homeland Security Presidential Directive No. 7 (HSPD-7) updated the policy of the United States and the roles and responsibilities of various agencies related to critical infrastructure identification, prioritization, and protection.

Jumping forward a few years, 2006 witnessed the creation of the National Infrastructure Protection Plan (NIPP) and the Critical Infrastructure Protection Advisory (CIPAC). The NIPP resulted in the establishment of Sector Coordinating Councils and Government Coordinating Councils to work together on furthering the protection and resilience of the critical infrastructure community under the authorities of CIPAC. The NIPP was revised in 2009 to reflect an evolution of the process, including expanded integration of all-hazard and similarly important principles.

Businesses are heavily focused on guarding their operations from interruption, preventing the loss of capital or intellectual property, and protecting public safety. They devote considerable resources toward maintaining their operations in the wake of a natural hazard or man-made threat, such as a cyberattack. Business owners and operators understand it is imperative that information infrastructure be well protected and resilient.

Cybersecurity is viewed as an essential aspect of risk reduction, just like risk management related to physical threats. Industry activities have included development of guides, road maps, and standards to improve security, operational safety, and reliability. Sector leaders undertake exercises, which the Chamber encourages, to assess and improve facility and system capabilities. In sum, private-sector owners and operators routinely strive to strengthen the security of their cyber systems and identify and mitigate any network vulnerability.

The businesses community already complies with multiple information security rules. Among the regulatory requirements impacting businesses of all sizes are the Chemical Facilities Anti-Terrorism Standards (CFATS), the Federal Energy Regulatory Commission-North American Reliability Corporation Critical Information Protection (FERC-NERC CIP) standards, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley (SOX) Act. Instead of adding to the regulatory burden, Congress should work to reduce the fragmented and often conflicting burdens that these different rules and bureaucracies place on industry.

More Regulation Would Impede Partnerships, Cybersecurity, and Innovation

The Cybersecurity Act of 2012 would authorize DHS to establish a regime for regulating the assets or systems of vital parts of the American economy. Given the discretion that government officials would have in designating "covered" critical infrastructure (CCI), the likelihood for DHS to regulate entities in many American communities is considerable. Instead of taking this less optimal route, the Chamber believes that policymakers should utilize and improve upon the sector-based risk assessments already being conducted by DHS.

Advocates of a regulatory CCI program argue, "We propose a 'light-touch' approach to regulation." However, the Chamber is concerned not only with the concept but with how it would be implemented. During the implementation phase of a regulatory CCI program, it would likely shift from being standards- and risk-based and flexible in concept to being overly prescriptive in practice.

A regulatory program would likely become highly rigid in practice and thus counterproductive to effective cybersecurity—due in large part to a shift in businesses' focus from security to compliance. Equally concerning, federal mandates could compromise security. By homogenizing security, our online adversaries would quickly learn to circumvent a company's protections and those of similarly situated companies.

It is not unreasonable to think that Congress, with the myriad issues on its plate, would find it challenging to maintain a level of vigilance necessary to ensure that the regulatory CCI program does not become prescriptive and detrimental to security. Contrary to some news headlines, the private sector routinely thwarts cyberattacks against its networks because it is fast and nimble in its response and recovery efforts. The Chamber is deeply concerned that a new regulatory regime would box in our critical infrastructures, hampering the freedom, agility, and innovation needed to deflect or defeat adversaries who are often quite amply resourced.

In addition to a regulatory CCI program, the Chamber is concerned about proposals that call on the owners and operators of CCI to develop risk mitigation plans that would be evaluated by a third-party auditor. Complying with third-party assessments would be costly and time consuming, particularly for small businesses. Most businesses already have processes in place for assessing and improving the strength of their networks, so added mandates are unnecessary if not misguided. Many in the business community are concerned that the release of proprietary information to third parties could actually create new security risks.

Also, the Chamber opposes any proposal requiring CCI to report any significant cyber incident to DHS or another government body. Information sharing is a two-way street, but this incredibly broad reporting threshold would be unworkable in practice and, perhaps, unhelpful because of data overload. From a fairness standpoint, legislative proposals lack any comparable requirement that government entities share threat information with CCI.

Policymakers Should Advance Collaborative, Sector-Based Risk Assessments

Over the past year, the Chamber has developed and worked with other industry organizations on cybersecurity proposals that offer positive and cooperative approaches to increasing U.S. information security and resilience.

The Chamber believes that policymakers should leverage and improve upon the sector-based risk assessments already being conducted by DHS or sector-specific agencies and industry under the existing NIPP. A key premise behind advocating collaborative sector-based risk assessments is to help answer a question that policymakers frequently ask: How are we doing on cybersecurity? Unfortunately, this question leads some to want to regulate the businesses community in prescriptive and unhelpful ways.

The Chamber has written a proposal advocating that DHS and industry sectors routinely produce a sector or subsector risk assessment that paints a picture of the strengths and vulnerabilities of the sector's cyber preparedness and resilience against a significant disruption, such as a cyberattack or a natural hazard. In contrast, the bill seems to use sector assessments as a springboard to increased regulation, rather than toward greater collaboration. Policymakers should ensure that the private sector and the federal government have done nearly everything they can within the public-private partnership framework to enhance U.S. cybersecurity before making a leap to an uncertain regulatory program.

Let's Boost Public Awareness

For several years, the Chamber has partnered with DHS and other agencies to increase businesses' knowledge of cybersecurity from an enterprise risk-management perspective. The Chamber has also promoted *Stop. Think. Connect.*, a public-private education and awareness campaign to help people stay safer and more secure online. But more needs to be done. We recommend heeding the example of government and industry mobilization in 2009 to halt the spread of the H1N1 flu virus. Simple and effective resources were made available to households, businesses, and schools across the country to mitigate the impact of the outbreak.

This collaborative effort could serve as a model for stemming much of the nefarious and comparatively unsophisticated activity seen online, freeing up limited human and capital resources to focus on more advanced and persistent threats. The Chamber recently partnered with the Federal Communications Commission (FCC) to unveil the FCC's new *Small Biz Cyber Planner*, a free online tool to help small businesses protect themselves from cybersecurity threats and make the price of attacks steep for their digital adversaries.

The Way Forward: Congress Should Enact a Meaningful Information-Sharing Bill

Cybersecurity is a significant economic and national security issue that the Chamber takes very seriously. We believe that the right path forward is for the public and private sectors to work together to solve challenges, to share information between network managers, and foster investment and innovation in cybersecurity technologies. The optimal way forward will not be found in layering additional regulations on the business community. New compliance mandates would drive up costs and misallocate business resources without necessarily increasing security.

Critical infrastructure owners and operators devote significant resources toward protecting and making resilient their information systems because it is in their overwhelming interest to do so. The Chamber urges Congress to support efforts that genuinely enhance collaboration between industry and government partners.

In addition, the Chamber supports information-sharing legislation that would address the need of businesses to receive timely and actionable information from government analysts to protect their enterprises by improving detection, prevention, mitigation, and response through enhanced situational awareness. The legislation should build on the recent defense industrial base (DIB) pilot project as a potential model for demonstrating how government cyber threat intelligence can be shared with the private sector in an operationally usable manner.

Businesses need certainty that threat information voluntarily shared with the government would be exempt from public disclosure and prohibited from use by officials in regulatory matters. Legislation needs to provide legal protection for companies that guard their own networks in good faith or disclose cyber threat information with appropriate entities, such as ISACs.

Once again, the Chamber greatly appreciates the opportunity to testify today. We look forward to working with you on these and other issues. Thank you very much.