CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

R. BRUCE JOSTEN
EXECUTIVE VICE PRESIDENT
GOVERNMENT AFFAIRS

1615 H STREET, N.W.
WASHINGTON, D.C. 20062-2000
202/463-5310

January 30, 2012

The Honorable Harry Reid
Senate Majority Leader
United States Senate
Washington, DC 20510

The Honorable Mitch McConnell
Senate Minority Leader
United States Senate
Washington, DC 20510

Dear Senators Reid and McConnell:

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, has serious concerns with both the substance of comprehensive cybersecurity legislation that may be considered by the full Senate in the next few weeks and the process by which committees of jurisdiction may be short-circuited by bringing this legislation directly to the floor without hearings or mark-ups.

Rushing forward with legislation that has not been fully vetted would be a major mistake. 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 infrastructures—from the shop floor to energy production and much more.

Since 2009, the Chamber has consistently said that it will support legislation that is carefully crafted and narrowly tailored toward effectively addressing the complex cyber challenges that businesses are experiencing. However, the Chamber strongly opposes new regulations and compliance mandates that would drive up costs and misallocate business resources without necessarily increasing security. More top-down regulations would significantly restrict necessary opportunities for the public and private sectors to work together collaboratively against our mutual adversaries.

Additional Regulation Would Hinder Partnerships, Cybersecurity, and Innovation

The Chamber has been working closely with Congress for nearly three years to develop smart and effective cybersecurity legislation. Threats that the private sector and government are grappling with daily in cyberspace are impacting them in real time and are constantly changing, making the need for speedy, public-private partnerships more important than ever. The Chamber believes that legislation should not impede security or the innovation that produces effective security technologies. Legislation needs to advance policies that truly protect industry and improve our nation's resilience.

More controversial issues—which are summarized below—need further debate and consideration in Congress, including an airing of costs to taxpayers, as well as with affected

industries before there is action on the Senate floor. In some cases, the Chamber has a fundamentally differing view than some in Congress who contend that regulations will eliminate our nation's cybersecurity challenges. Regulations are not a panacea and, in fact, could make improving cybersecurity more difficult.

- **Regulating "covered" critical infrastructure (CCI) and forced incident reporting:** At the time of writing, current proposals would authorize the Department of Homeland Security (DHS) to establish a regime for regulating the assets, systems, or operations of vital parts of the American economy. Given the discretion government officials would have in designating critical infrastructure as "covered," the likelihood for DHS to regulate entities in many American communities is considerable. Instead of taking this route, the Chamber believes that policymakers should utilize and improve upon the sector-based risk assessments already being conducted by DHS (or a sector-specific agency) and industry under the National Infrastructure Protection Plan. Current legislative proposals use sector assessments as a springboard to increased regulation, rather than toward greater collaboration. The Chamber believes that a regulatory program would become highly prescriptive in practice and thus counterproductive to effective cybersecurity—due in large part to a shift in businesses' focus from security to compliance. In addition, the Chamber opposes any proposal requiring CCI to report any significant cyber incident to DHS or another government body. Information sharing requires 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.

- **Mandating third-party audits:** 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.

- **Regulating the IT supply chain:** The Chamber is concerned that proposed legislation calling for prescriptive federal mandates on information technology product providers would lead to one-size-fits-all outcomes or to artificially chosen technology winners and losers. A regulatory framework would also slow the government's adoption of the latest and most secure technologies. Most troublesome, new procurement regulations tied to the supply chain would embolden foreign governments to react by promulgating their own cybersecurity standards regimes, which could act as a market barrier or lead to a balkanized and less secure cyberspace.

- **Adding to the regulatory bureaucracy:** American businesses already adhere to 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 in a bipartisan way to reduce the fragmented and often conflicting burdens that these different rules and bureaucracies place on industry. New legislation should not create parallel or duplicative authorities to address cybersecurity threats and vulnerabilities as businesses tend to prefer working with a single agency. In addition, it should not add new costs to the federal budget through the creation of unnecessary offices or positions.

- **Creating a uniform federal data breach rule:** In today's tough economy, businesses depend more than ever on having beneficial and trusted relationships with their customers. Thus, protecting sensitive personally identifiable information from theft or illegal uses has been and will continue to be a top priority for the business community. The Chamber, therefore, supports the enactment of a truly uniform federal standard for breach notification that is consistent with the best approaches in state law, which would ease compliance and foster job creation because businesses will be able to free up resources devoted to complying with a patchwork of nearly 50 state rules. To be workable and effective, any such legislation must recognize that both consumers and U.S. businesses are victims of crimes that give rise to a data breach. The legislation should contain carefully drafted provisions, including—but not limited to—preemption, liability, and enforcement provisions. If consistent with these recommendations, federal data breach legislation could join proposals that have earned a consensus of support among Chamber members.

Cybersecurity legislation should assist businesses with access to timely and useful information to prevent, deter, and mitigate an array of cyber threats coming from illicit actors. The Chamber will also consider legislation to spur research and development (R&D) activities, reform the Federal Information Security Management Act (FISMA) of 2002, encourage international cooperation against cybercrime, and boost public education around online safety and security, which we outline below.

- **Improving information sharing and legal protections:** The Chamber supports specific House legislation (H.R. 3523) 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 builds 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.

- **Spurring national cybersecurity R&D:** The Chamber urges Congress to leverage existing public-private partnerships to create a cybersecurity R&D plan that supports national (not simply government) priorities and includes a realistic road map for implementation, such as how to transition the benefits of research into operational environments. Organizations like the National Institute for Standards and Technology need to ensure the U.S. government's—as well as the private sector's, where appropriate—participation in the development of international cybersecurity standards and best practices. The Chamber also advocates increasing and making permanent the R&D tax credit, which can serve as a means of encouraging companies to increase their investments in cybersecurity.

- **Reforming the Federal Information Security Management Act of 2002:** The federal cybersecurity landscape has changed since FISMA was first enacted in 2002. Among other things, there is a strong need to harmonize information security programs across civilian government agencies. A reformed FISMA would help the government shift from a snapshot-in-time approach to information security to one that continually monitors servers and computers for weaknesses. Above all, the government needs to lead by example and work toward securing its own computers and information systems.

- **Encouraging international cooperation against cybercrime:** The Chamber supports Senate legislation (S. 1469) that constructively identifies foreign countries which need assistance with building capacity to battle cybercrime or which fail in ensuring the free flow of electronic commercial information within their borders. S. 1469, designed to be more of a "pep talk" than punitive, allows the President to identify certain countries of concern and fashion bilateral action plans to strengthen their legislative, institutional, and enforcement mechanisms.

- **Raising 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.

Congress Needs to Help Strengthen Collaborative, Public-Private Partnerships

Businesses strive to stay a step ahead of cybercriminals and protect potentially sensitive consumer and business information by employing sound risk-management principles. 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 takes the issue of cybersecurity very seriously, and we believe that the best solution to improving America's cybersecurity will not be found in additional regulation. Instead, legislation should support efforts that genuinely enhance collaboration between industry and government partners and that foster mutually agreed-upon solutions targeted at increasing collective security. Layering new regulations on critical infrastructure will harm public-private partnerships, cost industry substantial sums on compliance, and not necessarily improve economic and national security.

The Chamber looks forward to working with you on these important issues. However, we remain concerned that the legislation that could be considered by the Senate in the near term is a moving target. Cyber legislation needs to be examined by Congress through the regular hearing and mark-up process, not simply brought to the Senate floor. The incomplete, continually evolving draft bills that have been released to this point are an insufficient basis from which Congress, the Administration, or the business community can adequately assess their potential impacts on vital segments of the American economy.

Sincerely,

R. Bruce Josten

cc: Members of the United States Senate