Thomas J. Donohue
President and CEO
United States Chamber of Commerce
1615 H Street NW
Washington, DC 20062 February 9, 2012

Dear Mr. Donohue:

Thank you for the Chamber's letter regarding the Senate's efforts to prepare cyber security legislation to protect our nation from the malicious cyber activity that poses such a significant threat to our national security and our economy.

Beginning in 2009, the Senate undertook a cross-committee, bipartisan effort to develop comprehensive cyber security legislation in response to a threat that we recognize as significant, growing, and urgent. Malicious cyber activity poses one of the most profound threats to our nation; yet, our government currently lacks a framework with which to confront this threat. To put it candidly, we are playing catch-up in an increasingly costly – and potentially deadly – game.

I was struck by the testimony of the leaders of our Intelligence Community at recent Intelligence Committee hearings. Director of National Intelligence James Clapper called cyber security "a profound threat to this country, to its future, its economy, and its very being." And Robert Mueller, Director of the Federal Bureau of Investigation (FBI), stated that, "stopping terrorist attacks with the FBI is the present number one priority, but down the road, the cyberthreat, which cuts across all programs, will be the number one threat to the country." Think about that: in the years to come, malicious cyber activity will pose a threat to our country *greater than terrorism*. We simply cannot afford to repeat the mistakes of the past by failing to prepare for the leading threats of the future.

Yet, addressing cyber security is not simply a matter of staving off a future threat; it demands that we stop the hemorrhaging of national security secrets, intellectual property, and jobs already underway. In a recent letter to Senate Republican Leader McConnell and myself, eight former high-ranking national security officials led by Secretary of Homeland Security Michael Chertoff and Secretary of Defense William Perry pointed out that, not only are critical infrastructure such as power plants and hospitals at risk; moreover, "foreign states are waging sustained campaigns to gather American intellectual property – the core assets of our innovation economy – through cyber-enabled espionage." They counseled that the "constant barrage of cyber assaults has inflicted severe damage to our national and economic security, as well as to the privacy of individual citizens. The threat is only going to get worse. Inaction is not an acceptable option."

With such high stakes, it is essential that we produce legislation that is carefully considered and adequate to meet this challenge. To that end, I wanted to take some time to respond directly to your concern that the Senate may be "rushing forward with legislation that has not been fully vetted," since it appears that you may not be aware of the extensive, cross-jurisdictional, and bipartisan process that has guided the development of cyber security legislation for nearly three years now.

Your letter noted that "cyber legislation needs to be examined by Congress through the regular hearing and mark-up process," and I couldn't agree more. Since beginning our work on cyber security legislation in 2009, the Senate has:

- Held more than 20 hearings across at least seven different committees specifically on cyber security and related legislation, and addressed critical questions relating to cyber security in dozens of additional hearings;
- Held numerous briefings for Senators and staff on cyber security, including a briefing for all Senators by senior Administration officials last week;
- Organized several other forums for Senators to examine cyber security issues, including the Intelligence Committee's 2010 Cyber Security Task Force and an ongoing informal discussion group led by Senators Whitehouse, Blunt, Mikulski, and Kyl;
- Considered nearly twenty separate cyber security bills and numerous cyber security-related amendments; and
- Held mark-ups of cyber security legislation in five separate committees, each of which occurred under each committee's rules for regular order.

There is no question that the Senate has considered cyber security legislation as thoroughly and as conscientiously as any legislation in many years. As the non-partisan Commission on Cyber Security for the 44th Presidency concluded, jurisdictional responsibilities for cyber security in Congress are fragmentary and overlapping, and no single committee in Congress – nor any single agency or department in the executive branch – has an adequate view of the full sweep of cyber security policy. For that reason, in addition to the extensive consideration of legislation by individual committees, Leader McConnell and I agreed to establish a process wherein committees would work across jurisdictional lines, in "working groups" that included half a dozen different committees, to overcome parochial biases and develop legislation that is truly in the best interests of our nation's security. These working groups began actively meeting last July, and have worked arduously to develop legislation.

As part of this process, I have been clear, as outlined above, that these working groups must solicit and incorporate input from a wide range of non-governmental stakeholders – including leading industry representatives, academics, and security practitioners – as they developed the bill. There has been a vigorous dialogue with a broad community of stakeholders, and I am pleased to note that literally *hundreds* of changes to the legislation have been made so far as a direct result of private sector input. And as you note in your letter, the Chamber itself has been "working closely with Congress for nearly three years to develop smart and effective cybersecurity legislation."

While I am pleased that this three-year-long process has helped the Senate assemble legislation that represents substantial and productive input from such a wide range of stakeholders, our process is not yet complete. Given the complexity and significance of the legislation, it is essential that we have a thorough and open debate on the Senate floor, including consideration of amendments to perfect the legislation, insert addition provisions where the majority of the Senate supports them, and remove provisions if such support does not exist. For that reason, I have

committed to my colleagues that we will have an amendment process that will be fair and reasonable.

As you can see, far from being rushed, this legislation will have been subject to as fair, thorough, an open a process as is conceivable. It has been developed through a process about which Leader McConnell and I have consulted and agreed at every step. And I am convinced that the bill will be better for it.

I also appreciated hearing the Chamber's views on the substance of the legislation. Many of the issues you raised are concerns we have heard from others in the private sector, and the drafters of the legislation have painstakingly worked over the past few years to address these concerns. As you review updated drafts of the legislation, I expect that you will find most of the issues raised in your letter have been addressed.

Much attention has focused on provisions to ensure cyber security within a narrowly defined group of critical infrastructure assets: systems which, if disrupted or destroyed by cyber attack, would significantly damage United States national security and potentially cost thousands of innocent lives. Without some ability to intervene – in a targeted and efficient way – to ensure a certain level of protection in this narrow set of key infrastructure, the government cannot adequately protect its citizens. On the other hand, you are absolutely right that a regulatory framework creating bureaucratic redundancy, over-intrusive requirements, and unmanageable costs is counterproductive and contradictory to the spirit of public-private partnership that must drive our nations' cyber security efforts. It is precisely for that reason that the Senate has worked closely to develop a critical infrastructure framework that: (1) is outcome-based rather than prescriptive in order to preserve and foster private sector innovation; (2) is flexible enough to allow the government to work through existing mechanisms and relationships; (3) is narrowly tailored to focus on only the most sensitive and essential systems; (4) minimizes duplication of effort and bureaucratic redundancy; (5) directs the government to act *only* when market incentives have failed to create adequate security conditions; and (6) incorporates the private sector as a full partner in securing cyberspace. And the Information Technology Industry Council agrees that the latest critical infrastructure draft is a "careful delineation of the appropriate scope of cybersecurity-related regulation that will preserve and promote our industry's ability to innovate."

The Chamber's letter states that, "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 experience." I have no doubt that you are sincere in that commitment and I look forward to working in close cooperation with you to pass the Senate's carefully crafted and narrowly tailored cyber security legislation when it comes to the Senate floor in the next few weeks. Again, I appreciate your input into this vitally important legislation.

Sincerely,

HARRY REID