United States Senate

WASHINGTON, DC 20510

July 27, 2012

Thomas J. Donohue
President and Chief Executive Officer
U.S. Chamber of Commerce
1615 H Street, NW
Washington, DC 20062

Dear Mr. Donohue:

We are deeply disappointed with the Chamber of Commerce's mischaracterizations about the revised Cybersecurity Act of 2012 (S. 3414) that were included in a letter the Chamber sent to the United States Senate this week.

We are baffled that the Chamber opposes our voluntary, incentives-based approach to protecting our nation's critical infrastructure. A voluntary framework as proposed in the Cybersecurity Act of 2012 is the very framework your organization has championed. This approach was included as a recommendation in the March 8, 2011, white paper entitled "Improving our Nation's Cybersecurity through the Public-Private Partnership," coauthored by the Chamber and other industry groups. The recommendation stated, "government and industry must develop a menu of market incentives that government can put in place to motivate companies to voluntarily adopt additional security practices and technology investments." We have moved to a voluntary approach after extensive discussion with your organization, other private companies, and other members of the Senate.

In another example, your letter expresses concern that S. 3414 would eliminate the ability of non-civilian federal entities such as the Department of Defense and the National Security Agency to receive cybersecurity information directly from the private sector, including your membership. Section 707(a)(4) of S.3414 makes clear that such existing and future information sharing can continue if members of the Chamber want to continue to send information directly to the NSA. The attached document corrects other significant mischaracterizations your letter made about S. 3414.

Over the course of the last three years, as we have worked toward a compromise on cybersecurity legislation, the threat of a cyber attack against our country has grown even more serious. Now is the time for the Senate to finish this legislation, so the country can begin addressing its cyber vulnerabilities. Given the cyber attacks that have affected the Chamber's own control over the information of its members, we would have hoped that you would have an appreciation for the threat to the national and economic security of our nation. With this new approach, we believe that organizations like yours should support the legislation, and we are

hopeful that the information we are providing demonstrates that your characterizations and concerns are unfounded.

We met with Chamber representatives earlier today and have solicited input in the form of specific legislative text. We remain hopeful that you will partner with us in this important work.

Sincerely,

Joseph I. Lieberman
Chairman
Senate Committee on Homeland Security
and Governmental Affairs

Susan M. Collins
Ranking Member
Senate Committee on Homeland Security
and Governmental Affairs

John D. Rockefeller IV
Chairman
Senate Committee on Commerce
Science, and Transportation

Dianne Feinstein
Chairman
Senate Committee on Intelligence

RESPONSES TO THE CHAMBER OF COMMERCE'S LETTER ON S. 3414

CLAIMS	FACTS
While the program is being characterized as "voluntary," and participating entities may receive limited protection from punitive damages resulting from a cyber incident, the standards could be used to impose new obligations on participating companies.	**S. 3414 creates a voluntary, incentives-based program for companies that decide to adopt cybersecurity practices. No provision in S. 3414 makes these cybersecurity practices mandatory. S. 3414 does ensure that it in no way impacts existing regulatory authority for cybersecurity, but it does nothing to expand it. The bill is not designed to weaken existing regulatory authority.**
[T]he government would have the authority to modify or amend the standards developed through public-private collaboration, which would shift during the implementation phase from being flexible in concept to being overly prescriptive in practice.	**Because these standards are voluntary, there is no interest within the government for them to be "overly prescriptive." It is in the government's interest for the standards to be flexible and achievable. It will be the private sector's responsibility to create the standards and a company's responsibility to determine how to achieve them. Throughout the process, it will always be a company's choice to implement the standards. The cybersecurity practices are completely voluntary.**
The Chamber is also concerned that owners and operators of critical infrastructure would be evaluated by third-party auditors to demonstrate that they are in compliance with "all applicable cybersecurity practices," which could be unbounded in scope. Many in the business community are concerned that the release of proprietary information to third parties could create new security risks. Complying with third-party assessments would be costly and time consuming, particularly for small and mid-sized businesses, taking away resources that are dedicated to improving security. Businesses have processes in place for assessing and improving the strength of their networks, so added mandates are unnecessary if not misguided.	**S. 3414 does not require companies to use third-party auditors to demonstrate that they are in compliance with "all applicable cybersecurity practices." Companies can choose to use third-party auditors, or they can self-certify. It is their choice. Again, it is also their choice to decide whether to implement the cybersecurity practices in the first place.**

CLAIMS	FACTS
The "Marketplace Information" provision is ultimately designed to compel businesses that suffer a cybersecurity event to publicly disclose the occurrence. This part of S. 3414 aims to "name-and-shame" companies and could compromise their security. The Chamber strongly rejects mandating businesses to publicly disclose sensitive security information. Further, a letter from the Securities and Exchange Commission to the Senate last June indicated that investors have not asked for more disclosure in this area.	**The "Marketplace Information" provision: (1) instructs the SEC to evaluate whether it should make existing staff guidance on information security risks more formal; and (2) requires the SEC to provide Congress with a report on the types of information security risks that companies have disclosed to investors. To make informed investment decisions, investors must have quality information about material risks that face the companies they invest in. The SEC issued staff guidance on this issue in October 2011, in response to the letter the Chamber references, after finding that then-current SEC filings did not provide investors sufficient information on these risks. This provision merely asks the SEC to evaluate that staff guidance and creates no new authority for the SEC.**
Title VII of S. 3414 anchors too much control of information-sharing processes in the hands of the Department of Homeland Security. The department should have a role to play in facilitating and ensuring that cybersecurity threat information is shared in as close to real time as possible with appropriate government and business entities. However, S. 3414 would eliminate the ability of noncivilian entities such as the Department of Defense and the National Security Agency to receive cybersecurity information directly from the private sector. Information sharing legislation should not create silos that would diminish the timeliness and quality of threat data exchanged between businesses and government (and vice versa). Also, the liability protections related to information sharing in S. 3414 are not as clearly stated and direct as compared to competing measures.	**Nothing in this bill would prevent private companies from sharing information, as they do now, with DOD or NSA. In fact, the bill specifically states that existing relationships are unaffected.** **Title VII gives new authority for the government to receive information from the private sector. Because of this, Title VII must carefully balance the privacy and civil liberties that Americans hold dear with the need for real-time information sharing about cybersecurity threats.** **Whether in DHS, or another civilian agency, cybersecurity exchanges would serve as entry points for narrowly defined cybersecurity threat information. Similarly, an organization like the Financial Services Information Sharing and Analysis Center (FS-ISAC) could be designated to serve the same function.** **This bill delicately balances privacy and civil liberties concerns while ensuring that the government can help defend the country by receiving relevant information in real-time.**