United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Opening Statement of Chairman Joseph Lieberman
"Securing America's Future: The Cybersecurity Act of 2012"
Homeland Security and Governmental Affairs Committee
February 16, 2012
As Prepared for Delivery

The hearing will come to order, good afternoon. This is the 10th hearing our Committee has held on cybersecurity and I hope it is the last before the comprehensive cybersecurity bill before us today is enacted into law.

The fact is that time is not on our side.

To me it feels like Sept. 10, 2001. The question is whether we will act to prevent a cyber 9/11 before it happens instead of reacting after it happens.

The reason for this legislation is based in fact. Every day rival nations, terrorist groups, criminal syndicates and individual hackers probe the weaknesses in our most critical computer networks, seeking to steal government and industrial secrets or to plant cyber agents in the cyber systems that control our most critical infrastructure and would enable an enemy to seize control of a city's electric grid or water supply system with the touch of a key from a world away.

The current ongoing and growing cyber threat not only threatens our security here at home, but it is right now having a very damaging impact on our economic prosperity. Extremely valuable intellectual property is being stolen regularly by cyber exploitation by people and individuals and groups and countries abroad. It is then being replicated without the initial cost done by American companies. This means jobs are being created abroad that would otherwise be created here.

So when we talk about cybersecurity, people naturally focus on the very real danger that an enemy will attack us through cyberspace, but as we think about how to grow our economy and create jobs again, I've come to the conclusion this is one of the more important things we can do to protect the treasures of America's intellectual innovation from being stolen by competitors abroad.

Last year a very distinguished group of security experts, led by former Department of Homeland Security Secretary Mike Chertoff and Defense Secretary Bill Perry issued a stark warning:

"The constant assault of cyber assaults has inflicted severe damage to our national and economic security, as well as to the property of individual citizens. The threat is only going to get worse. Inaction is not an acceptable action." I agree.

The bill before us today is the product of hard work both across party lines and committee jurisdictional lines. I particularly want to thank my colleagues Senator Collins and Commerce Secretary Jay Rockefeller and Intelligence Committee Chairman Dianne Feinstein for all their hard and cooperative work in getting us to this point. We're going to be privileged to hear from all three of them shortly.

I also want to thank Senator Carper for his significant leadership contributions to this effort.

And I want to thank the witnesses who are here. We've chosen the witnesses deliberately because they hold differing points of view on the problem and on the legislation we've drafted and the challenges we face. We look forward to their testimony.

The Cybersecurity Act of 2012 does several important things to beef up our defenses in the new battleground of cyberspace.

First, it ensures that the cyber systems that control our most critical, privately-owned and operated infrastructure are secure. That's the key here—privately owned and operated cyber infrastructure can well be and probably someday will be the target of an enemy attack. Today it is the target of economic exploitation and we've got to work with the private sector to better secure those systems, both for their own defense and for our national defense.

In this bill, the systems that will be asked to meet standards are defined as those that if brought down or commandeered would lead to mass casualties, evacuations of major population centers, the collapse of financial markets, or significant degradation of security. So this is a tight and high standard. After identifying the systems that meet those standards, under the legislation, the Secretary of Homeland Security would then work with the private sector operators of the systems to develop security performance requirements.

Owners of the privately owned cyber systems covered would have the flexibility to meet the performance requirements with whatever hardware or software they choose, so long as it achieves the required level of security. The Department of Homeland Security will not be picking technological winners or losers and there's nothing in the bill that would stifle innovation. In fact, a letter from Cisco Systems and Oracle, two of our most prominent IT companies concludes that this legislation "includes a number of tools that will enhance the nation's cybersecurity without interfering with the innovation and development processes of the American IT industry."

Under our legislation, if a company can show the Department of Homeland Security that it already has high cybersecurity standards then it will be exempt from further requirements under this law. Failure to meet the standards will result in penalties that will be determined by the Department during the rulemaking and comment process.

It also creates a streamlined and efficient cyber organization within DHS that will work with existing federal regulators and the private sector to ensure that no rules or regulations are put in place that either duplicate or are in conflict with existing requirements.

The bill also establishes mechanisms for information sharing between the private sector and the federal government and among the private sector operators themselves. This is important because computer security experts need to be able to compare notes to protect us from this threat. But the bill also creates security measures and oversight to protect privacy and preserve civil liberties. Privacy and civil liberties advocates have indicated that our bill provides some of the best privacy and civil liberties protections of the various proposals being discussed in Congress.

The process by which we reached this cybersecurity legislation was very inclusive. We not only worked across committee lines, but reached out to people in business, academic, civil liberties and privacy, and security experts for advice on many of the difficult issues any meaningful piece of cyber legislation would need to address. I can tell you that literally hundreds of changes have been made to this bill as a result of this input and we think we've finally struck the right balance.

I briefly want to mention some things that are not in this bill. First and foremost, this bill does not contain a "kill switch" that would allow the President to seize or control part of or the entire internet in a national crisis. It's not there. It never was. But we put an exclamation point by dropping a section people thought included a "kill switch." It just wasn't worth it because of the urgent need for this bill.

There is nothing in this bill that touches on the balance between intellectual property and free speech that so aroused public opinion over the proposed "Stop Online Privacy Act," or the "Protect IP Act" and left many of my colleagues with scars or post-traumatic stress syndrome. In fact, this is not the ultimate verification of my

assertion that there's nothing like what concerned people with SOPA or PIPA, but I note with gratitude one of our witnesses, Mr. Stewart Baker, was a leading opponent of SOPA, but is testifying today in favor of our bill.

After the Cybersecurity Act of 2012 becomes law, the average internet user will go about using the internet just as they do today. But hopefully as a result of the law and outreach they'll be better equipped to protect their own privacy and resources from cyber attack.

The bottom line is a lot of people have worked very hard and in a very bipartisan way to face a real and present danger to our country that we simply cannot allow this moment to slip away from us. I feel very strongly that we need to act now to protect America's cyberspace as a matter of national and economic security.

Senator Collins.