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

Opening Statement of Chairman Joseph Lieberman
"Protecting Cyberspace: Assessing the White House Proposal"
Homeland Security and Governmental Affairs Committee
May 23, 2011
As Prepared for Delivery

Good morning. Thanks to everyone for being here, particularly the witnesses. If there is anyone who doesn't believe we urgently need to pass strong cybersecurity legislation, the topic of our hearing today, I would just ask them to look at some of the high-profile computer attacks that have happened in the past several months.

Let's take the Sony Corp. as an example. In two separate attacks, hackers stole the personal and billing information – including reportedly some of the credit card numbers – of 100 million people.

And when the site finally reopened last Thursday, the company found that it hadn't actually closed all the vulnerabilities that had been opened up in the wake of the first two attacks, and that hackers could still use the information to hijack people's accounts.

If that doesn't convince people we've got a real cybersecurity problem in America, consider the breaches that have occurred in the cyber systems of organizations that specialize in cybersecurity.

Take Oak Ridge National Laboratory, which has a very important role in the Department of Energy's mission to secure our electric grid from cyber attack, whether by enemy nations or cyber-terrorists. Oak Ridge was, itself, successfully cyber attacked just last month.

Or take a case that's been widely reported in the media: RSA, whose SecureID is used by some 40 million users in 30,000 companies - and parts of the federal government, including the Social Security Administration, the Department of Defense, and the United States Senate – had valuable security information stolen from its computers that could compromise these systems and actually be used in future attacks.

Bottom line, if we don't do something soon, the Internet is going to become a digital Dodge City. The internet is just too important to modern life to allow that to happen. This is a place that really calls out for law. It's time to say, if I may continue the Dodge City metaphor: "There's a new sheriff in town and we're going to have some law and order around here." We can do that without compromising, and in fact elevating, liberty and privacy.

The recent release of the White House's proposed Cybersecurity legislation is a very important step. I think it represents a turning point in our efforts to pass the strong measures we need to protect consumers, businesses, critical infrastructure and our national security from cyber attacks by terrorists, spies, or crooks.

I am pleased not just by the presence of the Administration's cybersecurity legislation, but by its substance. The President's proposal is similar in many ways to legislation this Committee has been working on in the past two Congresses. And where there are differences, I think we can work together to find agreement. In this regard, I'm very grateful to the witnesses for appearing before us today. This is the first time the Administration has testified on its cybersecurity proposal since it was released.

One important area of agreement is the recognition that the Department of Homeland Security must be given the job of protecting the dot gov and dot com domains. In other words, DHS will be the new sheriff in cyber town that we need.

A crucial part of this job will be for DHS to identify critical cyber infrastructure – the systems or assets that control things like power plants, electric grids and pipelines, which if commandeered by our enemies could lead to havoc, death, and destruction. DHS needs that authority and also the ability to evaluate the risks to those systems.

Once those systems and risks have been identified, the owners and operators of these systems should be required to develop plans to safeguard their systems. Those plans would need to be reviewed to ensure they will actually improve security – reviewed by DHS in our legislation, by government-accredited, third party evaluators in the White House proposal.

Just last week we saw an example of both why this kind of planning is so necessary and why DHS has raised itself to a quality where it deserves to have the job. A private researcher had discovered a major security flaw in a widely-used industrial control system and was going to present his research at a conference.

When personnel at DHS discovered this and explained to the researcher how dangerous it would be to have this information out in public before the security flaws had been patched, the researcher voluntarily canceled his talk.

As another cybersecurity expert said of this vulnerability: "This is different from simply stealing money out of someone's bank account. Things could explode."

Besides securing critical infrastructure, our bill and the White House bill would direct DHS to work cooperatively and on a voluntary basis with the private sector and state and local governments to share cybersecurity risk and best practice information. The White House proposal also clears the way for industry to share cybersecurity information without having to worry about running afoul of various privacy statutes that impede information sharing now.

The business and government communities would be free to use this advice as best suits their needs. There would be no "one-size-fits-all" mandates or dictates.

Both the White House bill and our committee bill also contain robust privacy oversight to ensure that our broader cybersecurity efforts do not impact individual privacy or civil liberties.

And, finally, both of our proposals would also reform and update the Federal Information Security Management Act to require continuous monitoring and protection of our federal computer networks and do away with the current paper-based reporting system.

One key difference between our bill and the White House proposal is that our legislation creates a White House Office of Cybersecurity with a Senate-confirmed leader. We just believe that the stakes are too high, when it comes to cybersecurity for our country, that whoever holds this position should be confirmed by the Senate and therefore be accountable to Congress.

Our bill would also clarify the President's authority to act in the event of a true cyber emergency, while at the same time ensuring that the President cannot take any action that would limit free speech or "shut down" the internet. In its original version this section was misconstrued, and we have tried to reassure everybody about the very, very limited circumstances under which the President could act, and the limited range of his actions. The Administration believes that additional statutory authority is unnecessary because the President has the authority that we gave him in this proposal already in existing law.

Bottom line, the internet is a thrilling new frontier with a plugged-in population nearly 2 billion users – and growing everyday – that has created a revolution in commerce, communications, entertainment, finance and government - really, just about every aspect of our lives.

But it need not—must not--be a lawless frontier, and I believe that with the proposals we have in front of us, we can bring about the needed change this year to make the internet safer and more secure.

The majority leader, Senator Reid, has taken a very active interest in this legislation. It remains a priority of his for this session. I've said to him that I believe it's the most important piece of legislation coming out of our committee in this session. He is working with the Republican leader, Senator McConnell, and there are six

different committees that claim some sort of jurisdiction over this subject matter. I believe it's the intention of Senate leadership to establish a process by which all those committees can, as quickly as possible, negotiate any remaining differences in the bills that have come out of committee so we can bring it to the Senate floor as quickly as possible.

We have had a very successful round of negotiations with the Commerce Committee, which is the other committee claiming major jurisdiction here, and we've resolved just about all of the differences that we had between us.

Now, before I turn this over to Sen. Collins, I wanted to take a moment to thank Phil Reitinger, who as Deputy Under Secretary for the National Protection and Programs Directorate, has done a great job in a relatively short period of time and really been a leader in the Administration in crafting this White House proposal, including working very productively and cooperatively with our Committee.

With the bill finalized, Phil has decided to move on to the next great chapter of his life. Phil, I want to wish you the best of luck and thank you for your public service, which has made a real difference to our country.

Sen. Collins.

-30-