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

Where we are, How Far We've Come

Cybersecurity Statement
July 31, 2012

Mr. President, as colleagues now turn their full attention to legislation to enhance our nation's cyber defenses, I want to take a few minutes to review where we are – because with the bill we now have on the floor, we are closer than ever to agreeing on a bill that can make our country more secure.

That said, we are eager to make further improvements to this bill, and to work toward a bipartisan solution. To do so, we need to begin processing amendments.

There are already more than 70 amendments filed, and more are on the way, so we don't have time to sit here staring at each other while we could be working through them.

We have a number of amendments we're ready to take votes on. But we of course need cooperation from both sides in order to nail down some votes on the first set of amendments so we can make progress.

But I also want to underscore that while there are important issues we need to work through this week, the reality is that because Senators on all sides have been willing to compromise, we have a golden opportunity to prove that we can work together when it counts the most.

And we can work in the tradition that led to our country's founding. I refer, of course, to that hot July day in Philadelphia, some 225 years ago, when this Senate was created as part of the "Connecticut Compromise" offered by two of my state's delegates to the Constitutional Convention – Roger Sherman and Oliver Ellsworth.

It passed by just a single vote but it helped keep the convention together because now the small states felt their interests would be protected and the large states knew they would have a greater say in the House of Representatives.

Not everyone got everything they wanted that day. But they found the middle ground that allowed them to go forward and finish writing our Constitution.

And this Senate – founded on compromise – runs on compromise. Compromise is not sand in the gears – it is the lubricant that lets us legislate.

Mr. President, that tradition of give and take – the ability to find the middle ground that allows us to move forward – has been crucial in our negotiations on the Cybersecurity Act of 2012.

What was once a chasm separating us is now a narrow ridge we're close to bridging and I firmly believe we will soon have a piece of cybersecurity legislation that can command an overwhelming "yes" vote in the Senate. And that will bolster our negotiating position when we conference with the House.

Let me show how far we've come.

Our side – which is reflected in the bill sponsored by myself, and Sens. Collins, Rockefeller, Feinstein and Carper - strongly believes that owners of critical infrastructure – the power plants, utilities and pipelines that if sabotaged or commandeered could lead to deaths and economic and environmental catastrophes –should be required to implement mandatory standards to protect critical cyber systems.

Other Senators – reflected in the SECURE IT Act sponsored by Senators McCain, Chambliss, Hutchinson and others, started this debate firmly convinced that the only thing we must do is enhance information sharing among government and the private sector.

If we all stuck to our guns, no legislation would have moved. But when it comes to cybersecurity, the status quo is not only unacceptable – it is dangerous. Some of our leading minds on national security have warned

that we are already losing billions of dollars a year to cyber spies and thieves, and could also face the equivalent of a digital Pearl Harbor or 9/11 if we don't shore up and defend our exposed cyber flanks.

Several of us met with NSA Director Keith Alexander just yesterday, and he warned us, again, that cyber systems that are critical to our nation's security remain vulnerable to attack. He said, and I am paraphrasing because this was behind closed doors, that we need this legislation to respond effectively to an attack on infrastructure as critical as Wall Street itself. And he said that today is like 1993 – when Al Qaeda launched a precursor attack on the Twin Towers. We all know they persisted and succeeded a few years later. He said our adversaries are testing us out.

General Alexander and officials from the Department of Homeland Security, DOD, and the FBI told us that they are working closely together, with well-defined roles and responsibilities, to leverage each other's capabilities. And they agreed we need to pass this legislation to give them more tools to work with one another and the private sector. We need to act. And I am convinced we will get there.

Thanks to additional work to bridge the divide chiefly by Senators Kyl, Whitehouse, Blunt, Coons, Coats and others we have come together and after a series of good faith negotiations have made major and difficult concessions in the interests of moving this legislation forward.

We now have broad agreement on a bill containing voluntary cybersecurity standards, along with compromises regarding information sharing that ensures privacy and civil liberties are protected, but still allow our defense and intelligence agencies the access they need to protect us.

Many advocates on both sides of issue think we have gone too far, or not far enough. But while advocates can hold fast in the perceived purity of their positions, legislators need to take all these deeply held views into account as we try to write law.

We have done that here, Mr. President, and I would like to, first, review our broad areas of agreement and then outline the differences that remain because I want my colleagues to understand how much progress has already been made.

Let me start with critical infrastructure

We now have broad agreement that the private sector should develop new cybersecurity practices to safeguard these facilities and that a new interagency council – consisting of the Department of Homeland Security, the Department of Defense, the FBI, the National Institutes of Standards and Technology and others – should review and approve these practices.

We have also agreed that adoption of these practices will be voluntary, that there will be no duplication of existing regulations or any new regulatory authorities, and that incentives need to be created – such as liability protection – to entice private-sector owners to adopt these practices once they have been developed.

The differences that remain, which we will hopefully work through in the next few days, really do pale in comparison to the gulfs we have already crossed. There are important issues still under discussion, and again I hope we can start voting on amendments as soon as possible to work through them. But we have already agreed to a lot.

Now let me talk about information sharing.

We agree that private-sector companies should be able to share cyber threat information with the government and each other under liability protections that incentivize sharing; that this sharing should be instantaneous and include technical, legal and oversight mechanisms to protect privacy; that existing information sharing relationships continue undisturbed, and that there should be no stovepipes among government agencies – agencies that need information should have access to it the instant it is provided to the government.

Some colleagues want more assurance that while a lead civilian agency will serve as the hub for immediate distribution of cyber threat information, it will do so without slowing down DoD or NSA abilities to access and act on that information. Others want to tweak the privacy protections a bit more. And we have already significantly strengthened the privacy protections thanks to Senators Franken, Durbin, Coons, and others.

But again, Mr. President, we're very close – it's a narrow ridge, not a chasm.

This is the Senate at its best. Shortly after the "Connecticut Compromise" was adopted at the Constitutional Convention, James Madison – often referred to as the "Father of the Constitution" – wrote that – and I'm paraphrasing here: "The nature of the senatorial trust" would allow it to proceed with "coolness," "system," and "wisdom."

These negotiations on the Cybersecurity Act of 2012 show that the Senate can put aside partisanship . . . move beyond gridlock . . . and fulfill our founders' vision of what this body can do when it comes to debating the great challenges of our time – with coolness, system and wisdom – and, if I could add, without rancor.

So over the next couple of days, let's debate all relevant and germane amendments, let's start voting where we need to, but then, for the good of our country, let us pass this bill so we can conference with the House when we return from the August recess – finalize the bill – send it to the President and defend our digital flanks against the kinds of attacks that are occurring as we speak.

I yield the floor.

-30-