Floor Statement for Sen. Joseph Lieberman
Introduction of Cybersecurity Act of 2012
Washington, DC
February 14, 2012

Mr. President, I rise today to introduce the Cybersecurity Act of 2012 and urge my colleagues to take it up and act on it quickly as a matter national and economic security.

First, I want to thank my friend and colleague on the Homeland Security and Governmental Affairs Committee, Ranking Member Susan Collins, and Commerce Committee Chairman Jay Rockefeller for all their hard work in putting together this bipartisan legislation.

I also want to thank Leader Reid for his unflagging support that helped us all work together across party and committee lines to pull this bill together.

Mr. President, I know it is February 14, 2012, but I fear that when it comes to protecting America from cyber-attack it is September 10, 2001, and the question is whether we will confront this existential threat before it happens.

We are being bled of our intellectual property everyday and would-be enemies probe the weaknesses in our most critical national assets – waiting until the time is right to cripple our economy or attack a city's electric grid with the touch of a key.

The system is blinking red. Yet, we fail to connect the dots – again.

Already top-secret defense technologies have been stolen, giving our enemies the chance to duplicate our weapons systems as well as learn how to defeat them.

Even the most sophisticated companies are being penetrated, and our adversaries are using information learned in one intrusion to plan the next, more sophisticated one.

Intellectual property worth billions of dollars has already been stolen, giving our international competitors access in the global market place without ever having to invest a dime in research.

In a report issued last year by the computer security firm MacAfee that studied 70 specific instances of data theft – including 13 defense contractors, six industrial plants and eight United States and Canadian government networks – former MacAfee Vice President Dmitri Alperovitch issued this ominous warning:

"I am convinced," he wrote, "that every company in every conceivable industry with significant size and valuable intellectual property and trade secrets has been compromised – or will be shortly – with the great majority of the victims rarely discovering the intrusion or its impact. In fact, I divide the entire set of Fortune Global 2000 firms into two categories: those that know they've been compromised and those that don't yet know."

Mr. President, if these examples aren't troubling enough, lurking out in the ether are computer worms like Stuxnet that can commandeer the computers that control heavy machinery and potentially allow an intruder to open and close key valves and switches in pipelines, refineries, factories, water and sewer systems and electric plants without detection by their operators.

Depending on the target or targets, this could lead to terrible physical destruction, mass evacuations, multiple deaths, and wide-spread economic disruption.

Owners of these critical systems have sometimes told us we don't need to worry about the security of their systems because they are not connected to the Internet. But late last year we found out just how wrong they are.

A Cambridge graduate student, using a search engine called Shodan that can locate industrial control systems linked to the Internet and identify the kinds of hardware and software being used, was able to identify more than 10,000 systems that could be vulnerable to fairly simple hacks.

"If a student can put this together, surely a nation state can do it," the student himself said.

The Department of Homeland Security was informed of these discoveries, and DHS worked with Computer Emergency Response Teams around the world to alert the owners of these systems that they were vulnerable.

Many of them said they had no idea they were connected to the Internet. In fact, we have been told by experts from across the government – in the civilian, military and intelligence communities – that a truly "air-gapped" system is as rare as a blizzard in the Caribbean!

If it exists, our best experts have yet to see it.

And Stuxnet has shown us that it doesn't matter if a system is air-gapped, because one thumb drive plugged into a computer can lead to infection.

Mr. President, if we don't act now to secure our computer networks, sometime in the near future we will be forced to act in the middle of a mega-cyber crisis. And in those situations, Congress rarely does its best work.

That's why it is essential we pass this bill now.

Let me tell you some of the important things this bill does to increase our cybersecurity.

First, it ensures that the computer systems that control our most critical infrastructure that are currently not secure are made secure.

Our bill defines critical infrastructure narrowly to include only those systems that if brought down or commandeered in a cyber attack would lead to a mass casualties, evacuations of major population centers, the collapse of financial markets, or degradation of our national security.

After identifying the precise systems that meet that definition of high-risk, the Secretary of Homeland Security would then work with that narrow slice of private-sector operators to develop cybersecurity performance requirements based on risk assessments of those particular industrial sectors. Owners would then have the flexibility to meet those performance requirements with whatever hardware or software they chose as long as it achieves the required level of security.

DHS will not be picking technological winners and losers. There is nothing in this bill that would stifle innovation.

And if a company already has met high security standards, it will be exempt from these requirements. The bill focuses on securing that which is not secure today – not on putting new requirements on companies that are doing all the things they should be doing to protect both themselves and our national security.

I want to stress, this only applies to those particular systems a company operates which could cause catastrophic damage. For example, let's say that Pepco, the electric company serving the Washington, DC, metro area, had systems that were deemed critical infrastructure covered under this bill. Only systems directly involved in the generation or distribution of electricity would need to conform to the increased security standards.

But Pepco's other systems, like human resources or customer service, are not covered by our legislation and would not be asked to do anything new.

However, once these kinds of improved security systems come on line, I can see that many companies would want to apply them to non-critical systems as a way to protect the privacy of their employees and customers, as well as giving these companies the chance to offer secure e-commerce services.

But that will be up to each company.

This bill seeks to make compliance easy for covered critical infrastructure operators by creating a more streamlined and efficient cyber organization within the Department of Homeland Security.

At each step in the process, DHS must work with existing federal regulators and the private sector to ensure no rules or regulations are put in place that either duplicate or are in conflict with existing requirements.

And if a company feels that the designation of its networks as critical infrastructure is in error, it will be able to appeal the decision through an internal complaint system the law requires DHS to set up, or they can go to federal district court.

This 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 – computer security experts need to be able to compare notes in order to protect us against the ever-evolving threat. But it also creates appropriate security measures and oversight to protect privacy and preserve civil liberties.

In fact, the American Civil Liberties Union has studied our bill and says it offers the greatest privacy protections of all the cybersecurity legislation that has been proposed.

Besides securing critical infrastructure, this bill does several other important things.

The bill provides for a cybersecurity research and development program to develop the new technologies we need to protect us from the ever-evolving cyber threats surely headed our way.

The bill also improves the security of the federal government's computer networks by cutting down on paperwork and moving to a system of continuous monitoring and "red-teaming" exercises to test for vulnerabilities.

And the bill strengthens the federal cybersecurity workforce by making sure we can offer competitive salaries so we can recruit and retain some of the best minds in the business.

Mr. President, let me address one myth about this bill that just doesn't seem to go away – and that is that it contains a "kill switch" that would allow the President to seize control of the Internet.

There is nothing remotely like that in this bill.

At one time we had considered language that would have limited sweeping powers we believe the President already has under the "Communications Act of 1934" to commandeer all electronic communications in times of war. It would have narrowly defined the President's authority, not given him unbridled power. But that provision was so widely misrepresented or misunderstood that we dropped it, rather than risk losing the chance to pass the rest of the urgently needed reforms contained in this bill.

I also want to make clear that nothing in this bill touches on issues that inflamed public consideration of the "Stop Online Piracy Act – or SOPA – or the Protect IP Act – known as PIPA.

This bill does nothing to affect the day-to-day workings of the Internet. Internet piracy and copyright protection are important concerns in the digital age. We need to deal with these legitimate concerns. But they are not part of this bill, and the average Internet user in the United States or abroad will go about using the Internet just as they do now after our bill becomes law.

I do want to address one complaint I've heard head on and that is that – quoting from a letter from the Chamber of Commerce – we are "rushing forward with legislation that has not been fully vetted."

We are not rushing this. This bipartisan legislation has been three years in the making and its outlines have not only been shared with stakeholders and the public, but their input has helped shape the final version of the bill before us today.

More than 20 hearings on cybersecurity have been held across at least seven different Senate committees, with dozens more held on questions relating to cybersecurity.

Since 2005, the Homeland Security and Governmental Affairs Committee alone has held eight hearings and will hold another one on Thursday where we will hear reactions to this bill.

Markups of cyber legislation have been held in five separate committees, each under the rules for regular order.

In the last Congress, both Homeland Security and the Commerce Committees passed comprehensive cybersecurity legislation that contains many of the ideas in this legislation.

And early in this Congress, Leader Reid and Minority Leader McConnell brought all the committees of jurisdiction together to form working groups that allowed us to work across jurisdictional lines to develop the bill we introduce today.

These groups have been working actively since last July and during that process – again – constantly reached out to industry, academics, civil liberties and privacy experts, and security experts. Hundreds of changes have been made to this bill as a result of their valuable input.

The legislation we introduce today has been thoroughly vetted. And Leader Reid has promised that when it comes to the floor it will receive a thorough debate and will be open to amendments to further improve the bill.

Mr. President, we have come so far with this bill. The threat it addresses is so clear and present. There is no reason for further delay. Time is not on our side. The threat is increasing exponentially and we are falling behind.

Let me quote from a letter sent January 2011 to Leader Reid and Minority Leader McConnell from a bipartisan group of eight of our nation's premier national security experts: former Bush DHS Secretary Michael Chertoff; former Clinton Defense Secretary William J. Perry; former Obama Deputy Defense Secretary William J. Lynn; former Bush Deputy Defense Secretary Paul Wolfowitz; former Bush Director of National Intelligence Admiral Michael McConnell; former Clinton Deputy Attorney General and member of the National Commission on Terrorist Attacks Upon the United States Jamie Gorelick; former national security advisor to both Bush Presidents and President Clinton, Richard Clarke, and former vice chairman of the Joint Chiefs of Staff, Marine General James Cartwright.

These leaders wrote: "[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."

I agree as do all my colleagues who have worked so hard to get this bill to the floor – and I again want to thank my friend and Ranking Committee member Susan Collins and Commerce Chairman Senator Rockefeller for all their hard work.

This legislation has the backing of Northrup Grumman, Microsoft, Entergy and numerous other groups.

Mr. President, if after all this time spent by the Senate working groups to reach a bipartisan consensus bill, and with all this support we now have from business, technology and other industry groups, we still do not act – we resign ourselves to live in a nation that is less

secure, to do business in an economy more vulnerable to theft and fraud, and to leave vital infrastructure exposed to destruction with the push of a button on a computer a world away.

I for one am not ready to cede this vital new frontier of cyberspace and the freedoms and economic opportunities that come with it to our enemies – the spies, the criminals and the terrorists who would hijack this tool of modernity and use it against as surely as they would turn airliners into guided missiles.

I urge my colleagues to pass Cybersecurity Act of 2012 and send the message to those who mean us harm that Americans are ready – as always – to fight for our freedom and security.

I yield the floor.