Thursday, June 10, 2010

MEMBERS OF THE SENATE HOLD A NEWS CONFERENCE ON THE PROTECTING CYBERSPACE AS A NATIONAL ASSET ACT OF 2010

TRANSCRIPT

June 10, 2010

NEWS CONFERENCE

MEMBERS OF THE SENATE

WASHINGTON, D.C.

MEMBERS OF THE SENATE HOLD A NEWS CONFERENCE ON THE PROTECTING CYBERSPACE AS A NATIONAL ASSET ACT OF 2010

Roll Call, Inc.
1255 22nd Street N.W.
Washington, D.C. 20037
Transcript/Programming: Tel. 301-731-1728
Sales: Tel. 202-419-8500 ext 599
sales@cqrollcall.com
www.cqrollcall.com

SENATORS HOLD A NEWS CONFERENCE ON THE PROTECTING CYBERSPACE AS A NATIONAL ASSET ACT OF 2010

JUNE 10, 2010

SPEAKERS: SEN. JOSEPH I. LIEBERMAN, I-CONN.

SEN. SUSAN COLLINS, R-MAINE

SEN. THOMAS R. CARPER, D-DEL.

LIEBERMAN: Well, good morning. And thank you for being here.

The Internet may have started out as a communications oddity some 40 years ago, but it is now clearly a necessity of modern life and sadly, one that is constantly under attack. And that's why we're here because we believe that it must be secured.

Today Senators Collins, Carper and I are introducing legislation which we are confident will do that, secure cyberspace. We call it the Protecting Cyberspace as a National Asset Act. I wish I could tell you it equals an acronym that you'll find it easy to say from here on in, but it doesn't. It describes what we're doing.

For all of its user-friendly allure, the Internet can also be a dangerous place with electronic pipelines that run directly into everything from our personal bank accounts to key infrastructure to government and industrial secrets. Our economic security, our national security, our public safety are all at risk as a result from new kinds of enemies with new kinds of names like cyber-warriors, cyber-spies, cyber-terrorists and cyber-criminals. And that risk may be as serious to our homeland security as anything we face today.

Computer networks at the Department of Defense, for instance, are being probed hundreds of thousands of times a day. Networks at the Department of State, Homeland Security, Commerce as well as NASA and the National Defense University have all suffered major intrusions by unknown foreign entities. Key networks that control vital infrastructure like the electric grid have been probed, possibly giving our enemies information that could be used to plunge America into darkness at the press of a button in a country far away from our borders.

Banks have had millions and millions of dollars stolen from accounts by cyber-bandits who are operating across oceans and have never been anywhere near the physical bank itself. In a report by a security company called McAfee, about 54 percent of the executives of critical infrastructure companies that were surveyed said their companies had been the victims of denial of service attacks or network infiltration by organized crime groups, terrorists or nation states.

These are very costly. The downtime to recovery from these attacks can cost as much as $8 million a day. Our efforts at securing these vital but sprawling government and private sector networks have been improving. But they remain disjointed, understaffed and under-financed.

President Obama has correctly described America's cyberspace as, quote, "a strategic national asset." But I would say -- and I -- and I know that Senator Collins and Senator Carper agree -- it is one that we have acted to protect without sufficient -- a sufficient sense of urgency. The fact is that our defenses, our national cyber defenses

are still catching up with those who are attacking our cyberspace.

So this bill which the three of us are introducing today would bring these disjointed efforts together. First, our legislation creates a National Center for Cyber-Security and communications, an NCCC, within the Department of Homeland Security run by a Senate-confirmed director who will have the authority and resources to work with the rest of the government to protect federal computer networks.

Thanks to great work by Senator Carper, our legislation also reforms and updates, FISMA, the Federal Information Security Management Act, to require continuous monitoring and protection of our federal networks. And it also does away with the paper-based reporting system that currently exists.

But obviously, our responsibility for cyber defense goes well beyond the public sector because so much of cyberspace is owned and operated by the private sector. Department of Homeland Security has actually shown that vulnerabilities in key private sector networks like utilities and communications could bring our economy down for a period of time if attacked or commandeered by a foreign power or cyber-terrorists.

But today the Department of Homeland Security -- in fact, our government -- lacks the power to do what it needs to do in response to get our economy back up. Our legislation, therefore, gives the Department of Homeland Security the authority to ensure that our nation's most critical infrastructure is protected from cyber attack.

Obviously, that will only be successful if industry and government are working together. So this legislation sets up a collaborative process where the best ideas of the private sector and government can be used to meet a baseline set of security requirements.

Of course, the Department of Homeland Security will need a lot of people to accomplish these missions. And our bill -- our bill gives it the flexibility to recruit, hire and retain those experts.

President Obama has created a cyber-security coordinator within the White House. And that's a good step in the right direction. But our bill takes it a next big necessary step. And that is to make the position permanent, transparent and accountable to Congress and the American people by creating a Senate-confirmed White House cyber-security coordinator whose job it will be to lead all federal cyber-security efforts, develop a national strategy to protect cyberspace and give policy advice to the president both in areas covered by the Department of Homeland Security and those covered by the Department of Defense or other agencies.

In the event of an attack on America's cyberspace or the threat of an attack that could have catastrophic consequences to our economy, national security or public safety, our legislation gives the president of the United States the authority to impose emergency measures on a select group of critical infrastructure cyber networks to preserve those networks and assets and protect our country and our

people. Those emergency measures would automatically expire within 30 days unless specifically renewed. I know there are a lot of questions about that, so I will be available to try to answer them.

Finally, our legislation would require the federal government to develop and implement a strategy to ensure that the almost $80 billion of information technology products and services that the federal government purchases each year are secure and do not provide our adversaries with a backdoor into our networks. In other words, to use the federal purchasing power to drive security innovations in information technology that will therefore be available to the private sector as well. To me this legislation is both obvious and urgent.

Cyberspace is today the -- the new frontline in our responsibility to protect the homeland security of the American people. There was recently a report by the bipartisan Center for Strategic and International Studies that concluded -- and I quote, "We face a long-term challenge in cyberspace from foreign intelligence agencies and militaries, criminals and others. And losing this struggle will wreak serious damage on the economic health and national security of the United States." Given these stakes, the three of us are confident that our colleagues will join with us across party lines and pass legislation this year to protect this particular part of our homeland security.

Senator Collins?

COLLINS: Thank you, Mr. Chairman.

Since the terrorist attacks of September 11, 2001, our nation has done a great deal to protect potential targets such as our seaports, our chemical plants and transportation systems. And indeed, our Senate Homeland Security Committee has spent a great deal of time identifying emerging threats and pinpointing vulnerabilities.

There is perhaps no greater vulnerability that we have yet to address than that of securing cyberspace. We cannot afford to wait for cyber-9/11 before our government finally realizes the importance of protecting our cyber resources.

The threat of a major cyber attack is very real. It is not a matter of if an attack will occur, but when. As intelligence officials have warned, malicious cyber activity is occurring each and every day on an unprecedented scale with extraordinary sophistication.

Just this March the sergeant at arms reported that the computer systems of Congress and executive branch agencies are now under cyber attacks an average of 1.8 billion times a month. Cyber crime also costs our national economy billions of dollars. As our national and global economies become more intertwined, cyber-terrorists have greater potential to attack high-value targets from anywhere in the world. They could disrupt our telecommunications systems, shut down electrical power grids or freeze our financial markets.

A cyber attack could cause billions of dollars in damage and put thousands of lives in jeopardy. This truly is a major national and

international concern and affects both the private sector and the public sector.

And that's why I'm very pleased to be joining my two colleagues today in introducing cyber-security legislation. Our bill would fortify the government's efforts to safeguard America's cyber networks from attack and would build a public/private partnership to promote national cyber-security priorities.

From our work on this issue we know that, as the chairman has pointed out, for far too long our approach to cyber-security has been disjointed, ineffective and uncoordinated. This simply cannot continue because the stakes are far too high. We need a comprehensive cyber-security strategy backed by aggressive implementation of effective security measures.

One of the most important provisions of our bill would establish an essential point of coordination for both the public and private sectors. And that is the Office of Cyberspace Policy in the executive office of the president and the creation of the new National Center for Cyber-Security and Communication within the Department of Homeland Security. I would note in coming up with the Cyber Center we looked at the National Counterterrorism Center within the Office of the Director of National Intelligence as a model.

We would also establish, as I mentioned, a partnership with the private sector to improve cyber-security across the nation. In cases where owners and operators are responsible for assets whose disruption could cost thousands of lives or billions of dollars the bill would mandate compliance with certain risk-based performance standards.

But I want to emphasize that those standards would be developed in collaboration with the private sector. And we do not dictate specific security measures. Rather, the center would establish risk-based performance standards, and then it would be up to the private sector to decide how best to meet those -- those standards.

Those requirements, for example, would apply to vital components of the electrical grid, telecommunication networks, financial systems and other critical infrastructure systems. The president would also have emergency authority under our bill. I want to point out, however, that it doesn't include the so-called kill switch. It is limited in duration and scope and carefully circumscribed.

The bill does not authority any new surveillance authority. So this isn't a case of the federal government increasing its surveillance of private sector computers. Nor would it permit the government to take over private networks. Rather, it enables the government in concert with the private sector to better protect our nation's cyber assets.

Let me close by quoting Denny Blair, the former director of National Intelligence, who warns the following. "The national security of the United States, our economic prosperity and the daily functioning of our government are dependent on a dynamic public and private information infrastructure which includes telecommunications, computer networks and systems and the information residing within

them."

He then said that this critical infrastructure is severely threatened. We cannot wait for the worst to happen, for a cyber-9/11, before taking strong action to address this growing vulnerability. Thank you.

LIEBERMAN: Thanks very much, Senator Collins.
Senator Carper?

CARPER: Thank you, Mr. Chairman. And my -- my thanks to you and to -- to our colleague, Susan, for -- for your leadership in bringing, not just together today, but together on an important issue.

A fellow that we've heard of before -- and I don't know if any of us ever met him -- a guy named Willie Sutton was once asked why do you rob banks. And he replied famously, "Because that's where the money is."

People today still rob banks in order to get our money. But they found other ways, safer, easier, simpler ways to get our money than -- than just robbing banks.

People today still try to -- to steal our intellectual property rights, whether it's trying to develop a new joint fighter, the F-35, whether it's trying to build advanced radar systems. We still have spies out there. They're still trying to get our military secrets.

They're still trying to get our intellectual property secrets. But they have another way to do it. And it's a lot simpler. And it's a lot safer. And it can be done remotely, almost leaving no trace.

The reason why we're here today working on this proposal is because times have changed. The nature of the threat has changed. The ability of people to get our money, to get our sensitive information, personal information, to be able to steal our military secrets, even to tap into the e-mails of -- of Secretary Robert Gates, Secretary of Defense Gates. That kind of thing couldn't have happened before. But it's happening today. And that's why we're here for this -- for this -- for this effort.

For some time our committee has been looking at how to secure cyberspace as our federal government from -- not only from current threats, but also from emerging threats. And we found that -- Susan and Joe both suggested we don't -- we're not very well coordinated.

We have the intelligence people working here. We have the military people working here. We have the homeland security people working here. We have other folks, the private sector, working over here. Nobody in the White House, nobody in the Department of Homeland Security is trying to coordinate our efforts. And under this legislation that would change.

As it turns out, we do spend a fair amount of money on this purpose. We do it in a way that's not very smart. We do it in a way that tries to ensure compliance. We do it through a paper process,

but we don't do it in a real way.

We used to do a similar kind of thing in protecting or nuclear power plants. They would go through a paper process to try to make sure that they were protected from -- from harm, from somebody trying to come in and do bad things at a nuclear power plant.

We don't do that quite that way any more. We have force on force exercises. We have people that are our guys, but they come in the guise of bad guys, trying to get into our nuclear power plants to do harm to the nuclear power plants and to disrupt what's going on there and to create threats to -- to the plant and to our -- our community. We are -- we need to take a similar kind of approach, not a paper-based approach to -- to ensuring security, but a real -- a real kind of approach and model it really after what we do with the -- our nuclear power industry.

I -- I -- I also want to mention that -- that -- and just to say thanks to our colleagues for accepting one of my proposals. And that is the proposal to create a -- a nationwide, a network of what we call cyber challenges. We all know about baseball. We know we have the major leagues. We have the minor leagues. We have the farm system. And eventually you try to work up through the farm system.

Over in China, places like that, they're -- I don't know if they play baseball, but they have a farm system. And their farm system actually takes people, young people who are interested in these kinds of issues -- how do I hack into somebody's system, either for fun or for profit. And they train them. And they have competitions. And they get better and better. And then they turn them lose on, among others, us.

We're going to emulate that approach. We call them cyber challenges. And the idea is to foster competition and innovation that's aimed at teaching young Americans a couple of things. But one is how to enhance our nation's cyber defenses and at the same time teach them how to protect their own systems from -- from -- from intrusion.

I think we need these cyber challenges to close the -- the gap between the number of so-called cyber-warriors being produced in China, in Russia, North Korea and other places and have more of them here home-grown. In my own state -- I'll close with this. But in my own state of -- of Delaware we pioneered these cyber challenges. I look forward to seeing how we stack up later this year in our national/international counterparts this summer when we do our first cyber challenge summer camps when they commence.

We've all been to summer camps before. This is a different kind of summer camp. And this is a summer camp that we need. And hopefully with this step we'll actually create them. Thank you.

LIEBERMAN: I feel like I should break into a chorus of See You in September, after summer camp.

We're happy to try to answer any questions you have.

Yes?

QUESTION: One of the major differences in bills moving for cyber-security responsibility outside of OMB is the office you created with the government Act and into DHS. Yet two years ago your committee and others really lambasted DHS for not being able to secure their own networks. Why the switch? They haven't necessarily gotten that much better, though they are better. But are they that much better now they can handle all the government?

LIEBERMAN: Yes.

QUESTION: It just seems an interesting move.

LIEBERMAN: Yes. Look, the first thing to say is that we all concluded that we had to put in one place the authority to protect the federal government cyber networks and the private networks as well from attack and that the Department of Homeland Security was the natural and logical place to put it because this is a department we created to protect our homeland security. And protecting cyberspace is a critical part of that.

I don't think any of us would say that DHS, Department of Homeland Security, thus far has been everything we would want in cyber-security. But there are a lot of reasons for that. And the good news is that it has really focused now over the last year or so on improving its capacity on new personnel. And this legislation would really give it the authority to do exactly what -- what we need somebody to do.

So we have -- we have confidence in the direction in which DHS is moving. We know that it's the logical place for this coordinating authority and protective authority to be. And we're confident that they can make it work.

Senator Collins?

COLLINS: Two points -- first, DHS has already done a great deal of work to identify critical infrastructure. And, in fact, has identified 18 sectors of -- of critical infrastructure. Therefore, a lot of work has already been done by DHS to identify essential assets across the country. And it's logical for DHS to use that work and further refine it to identify the critical cyber assets. So consider work already done by DHS.

Second, OMB's focus is not a security focus. It's a budget focus. And one reason why the current law has not been very successful, despite the extraordinary work that Senator Carper has done in pushing OMB, is because, as he indicated, OMB really just has a paperwork exercise that it goes through. It's far more important that the review of agency plans be done by a department whose mission is to protect the homeland.

LIEBERMAN: Thanks, Senator Collins.

Yes?

QUESTION: Will this bill help form a definition as to what constitutes an act of war in cyberspace? What about guiding principles that would form the legal and policy-based procedure operations?

LIEBERMAN: Well, it sets some principles. But -- but it doesn't really define in that sense an act of cyber-war. I know there's a lot of work going in within the new cyber command in the Defense Department and in the Defense Department generally to develop essentially strategic doctrine for cyber-war. These are very important. They're fascinating questions. And I don't want to go into them any more.

What -- that this does -- and perhaps I should use this moment to just talk about it a little bit because I know it's aroused interest. It does create an authority within the president of the United States in a national cyber emergency to take steps with regard to the private cyber infrastructure. And I -- I want to make clear that there's nothing in here that authorizes the government to, for instance, take over any cyber networks.

We -- we divide in this bill -- let me put it a different way. We identify in this bill or authorize DHS to identify what we called covered critical infrastructure. The most critical parts of our cyberspace, which if attacked could cause catastrophic consequences. And that's the -- what might that be particular parts of the electric grid or -- or the financial infrastructure grid or, for instance, a particular dam which is operated in a -- through the Internet.

And the federal government through the -- through DHS has the capacity to ask, working collaboratively to set up certain actions that these covered critical cyber infrastructure have to take. And then they receive a certification from DHS. This is not the majority of cyberspace. This is critical stuff.

If the federal government, if the president concludes that some part of that covered critical infrastructure is either under attack or about to be under attack, either separately or as part of a conflict that we're involved in with another nation or a -- or a -- for instance, a terrorist group, this bill gives the president the authority to take action that the private infrastructure might want to take but would be worried about taking on its own in part for fear of legal liability.

What am I talking about? The government -- the president might order a particular company or part of the infrastructure to put a patch on to protect or to stop a breach, if you will. It might order parts of a -- of a -- of a cyber network to refuse to accept any incoming, as it were, across cyberspace from a particular country.

So it's that kind of thing. And I want to say that one of the -- one of the things that we then say in this bill is that when a private company complies with the order of the president of the United States in such a critical national emergency, they are made immune from

liability for any consequences of that action. And that might otherwise make them hesitate to take action for fear of legal liability. But the president ought to have the authority in a moment like this to say no, we need you to stop everything coming in from country A or we need you to put this part of your network down for 12 hours or a day or whatever.

CARPER: Could I -- could I just...

LIEBERMAN: Please? Yes.

CARPER: Let me just use a moment to -- to use a military analogy that we -- I think we're all familiar with that helps describe in part what we're trying to do here. For a number of years in Iraq we deployed our troops. We sent them out in up-armored Humvees. They hit a roadside bomb, a lot of people got hurt, injured, killed.

We found out that if we'd send them out in MRAPs, they could go out and run -- literally run over a roadside bomb and because of the protection that the vehicle provided to our troops, they generally survived, sometimes not even -- with -- with no injury. What we -- one of the things we're trying to do with our legislation is to say when we're making investments in -- in information technology, why don't we provide like the MRAP, provide the protection for our system, in this case, for -- for our secrets just like we do with the MRAP provides protection for our troops. Why don't we buy something that actually gives our systems and our sensitive information that protection up front? Well, this legislation does that.

LIEBERMAN: Yes?

QUESTION: Senator, you mentioned the (inaudible). You mentioned earlier that you're confident that this -- you're (inaudible). Can you talk a little about your game plan moving this through (inaudible)?

LIEBERMAN: Yes.

QUESTION: You've got an indication from the -- from the Senate leadership they want this bill forward. How do you (inaudible) the proposal (inaudible)?

LIEBERMAN: Right. OK. So the good news about the two major bills put together are that they're bipartisan. Senator Rockefeller and Senator Snowe have one. And obviously, Senator Collins and Senator Carper and I have this other one. There are other committees that have particular pieces of legislation that relate to this that are not comprehensive. Judiciary has some. Armed Services has some. And I think we're very open to including those in this measure.

Here's the good news about this. Senator Reed, Senator Harry Reid is -- is very committed to doing something to -- to protect our cyber networks in this session of Congress. I will tell you that our committee has been working on this for some period of time. But a few months back, maybe a little longer than that, Senator Reid called a bunch of the chairmen in in relevant areas because he had just received a briefing on the cyber threat. He was very concerned about

it and said this is something I want to get done in this session of Congress.

We just by coincidence met yesterday. He's convened a process now where his -- his staff is going to coordinate among the staffs of the relevant committees. I would say that though there are differences between our approach and the Commerce Committee approach -- and needless to say we think our approach is better -- the differences are not irreconcilable. I think they're quite logically reconcilable.

And I -- I don't know whether Senator Collins wants to speak on this, but I've heard from people in the private sector who have talked to people in both parties, including the leadership of both parties, and they've been encouraged to believe that there really is an opportunity here because of the threat to our national security to have a bipartisan agreement.

Yes. Let me just tell you this. We spent a fair amount of time -- more time than probably the three of us wanted to spend -- in developing this legislation, spent a lot of time with public and private sector stakeholders. And you see some of this in the statements of support that we put in your packets today. So now that we're introducing this today, we're -- we're putting our foot on the gas pedal.

And next Tuesday we will hold a hearing on our committee on this bill. The following week, Wednesday, we're going to hold a markup in our committee. So hopefully, you know, by the week before we break for July 4th we will have reported this out of committee to the floor.

STAFF: Thank you all. Last question.

LIEBERMAN: I have to ask -- she has to have one, you know, because she has such longstanding.

QUESTION: I just have a question on DHS versus Commerce.

LIEBERMAN: Yes.

QUESTION: What kind of negotiating room do you think there is or there should be between where this should all come down? You sound pretty strong about DHS and you know all the (inaudible).

LIEBERMAN: Well, I do because, you know, DHS -- this is the job we gave the Department of Homeland Security. That -- this is its mission. And to put it elsewhere just doesn't make sense. And I think particularly some might say -- well, we've set up a very collaborative process. And I'm -- I'm very pleased. And you'll see that private sector groups are putting out statements of support for our proposal.

I'd also say this, Lita. Leading up to this introduction, our staffs have been working -- our staff, the three of us, have been working together with the staff of the Commerce Committee. And they've made some real progress, I think, in minimizing areas of -- of conflict. So -- but -- but -- but we're going to hold firm on the

basic principle here. We need to coordinate our cyber defense efforts. And the only logical place for that to be for the non-defense civilian, government networks and the private networks is the Department of Homeland Security.

Thank you all.

STAFF: Thank you, everybody. And staff will stay behind to answer technical questions, if you have them.

END

June 09, 2010 08:00 PM EDT

Roll Call, Inc.

Powered by InfoDesk