I have talked to so many small businesspeople in the last month as I have been out talking to people in my home State and in other States. What most of them say comes down to they just need to know what their tax liability is going to be, and they need to know it is going to stay that way for a while. That is how they make their plans. They do not want to hire someone if we are just going to have a 6-month fix or a 1-year fix or a 2-year tax policy. A 2-year tax policy is a nightmare for businesses because they cannot make a long-term plan. They can't have a strategy that puts three more people on the payroll and then have those costs go up at the end of that 2-year period.

It is important we give our businesses stability and that we show we understand they are the economic engine of America and that we want them to succeed and to hire people and give new jobs and get this unemployment rate well below the nearly 8 percent that it is now down into the 6-percent or 5-percent range.

Now, let's talk about the elderly. All of these years I have heard people talking about the importance of saving for retirement, and we have encouraged people to do that. The people who have done that are looking at a huge tax increase.

Madam President, I ask unanimous consent to speak for up to 10 more minutes.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mrs. HUTCHISON. These are people who have done the right thing. They have saved. They have tried to make sure they didn't need any kind of government handout. They have earned Social Security—and that is not a government handout—and they want to know they can make it living the lifestyle they want to live because they have saved. But here we are talking about raising their taxes on the dividends of any stock they might have invested or might have been in their company 401(k) plan, and we are talking about raising the capital gains rate.

In fact, the dividends rate could be as much as 39.6 percent. Nearly forty percent on dividends is going to kill a plan for retirement, and it is just not right to change the rules when we have had a lower dividend tax rate or capital gains tax rate for people who have done the right thing and saved for their own security. That is what will make a strong economy, and for our retirees to be able to get the rest they deserve.

What about married couples? One of my longstanding priorities in the Senate has been to make sure we have a level playing field on deductions of State and local taxes. Some States have income taxes, some States have sales taxes, some have both, and a few have neither. But for those who have both, we give them the choice of a sales tax deduction or income tax deduction. That means on their Federal income tax they don't pay taxes on the taxes they pay. If they are paying a State income tax or a State sales tax, they should be able to deduct at least one of those because there is no reason to be taxed on taxes. The sales tax deduction expired at the end of last year. If we don't renew it, the people who have sales taxes and no income tax are going to be severely disadvantaged.

In my home State of Texas, that makes at least a $500 difference to every person who takes those deductions. That can be a lot for 2 million Texans who claim this deduction, to have an average of $500 they are paying on taxes. So it is not a level playing field if we don't renew that extension. There are eight States that have no income tax, and they do have sales taxes. So I am hoping we will have that kind of parity in taxation, which we must do by the end of the year to allow that equity to take hold.

A second priority of mine is the marriage penalty. I passed the original amendment that would double the standard deduction for married couples. This has been a hugely popular tax deduction because in the past, when two single people got married, they would go into the higher bracket, and they would not get a double standard deduction. Prior to 2001, 25 million couples paid a penalty for being married, and the average cost to them was $1,400. As an example, if a Houston policeman, with a taxable income of $50,000, is marrying a data entry clerk who makes $30,000, they are going to have a tax increase of about $800 a year because the marriage penalty will come back at the end of this year.

We enacted relief in 2001. It was my amendment. And I hope we will not leave here December 31 of this year without renewing the marriage penalty tax relief. It will mean $800 for married couples, as an average, and, for sure, that is something they deserve when they get married. They shouldn't have to pay more for their decision to get married. So if we don't extend the tax cuts that are in place right now, at the end of this year we are going to see tax relief for the middle class, small businesses, family farms, retirees, and families go away. That relief will go away, and all of their taxes are going to go up. That is not even counting the surcharges that are going to take effect January 1 of next year in the health care law on dividends and capital gains.

So if the dividend rate goes back up to 20 percent, it is going to be 23.8 percent. If someone is in the 39.6-percent bracket, it is going to be 43.4 percent. So it is something we must deal with.

The other side of the equation is spending. Madam President, we must do something about the $1 trillion deficits we have had year after year after year that have made this debt go up from $10.6 trillion 4 years ago to $16.2 trillion today. We are about to hit our debt limit, and that means we are going to have to increase the debt that is already a wet blanket on this economy.

So, Madam President, we must come together.

We can do it. We can cut spending. We can address entitlement reform that will bring our entitlements into an actuarial soundness. Social Security and Medicare have already sustained enormous cuts in the health care plan that was adopted 2 years ago, and we can't sustain either of those programs if we continue to go in the direction we have been going.

So rather than the sequestration—which is going to take more than $1 trillion out of federal programs, half of which is going to come from defense—we have got to do something about it now.

We have a 10-year plan that could cut the deficits. But we have got to do more. We have got to enact the next step in budget cuts, and it has got to include entitlement reform, in my opinion. I know there are disagreements about that, but that is the argument and the discussion we need to have. It is our responsibility.

We should be using this time—today, tomorrow, this week—to start putting together a framework of discussions, because we will be in session from the end of November probably up until right before Christmas, and the American people deserve to have a solution, something that assures small business that they can count on a tax structure that is fair, that can allow them to make a reasonable profit, and allow them to hire more people.

We have got to cut spending so we can manage this government in a responsible way without it encroaching on the vibrancy of our economy. That is our challenge. I hope this Congress is up to it.

Madam President, I yield the floor.

CYBERSECURITY ACT OF 2012

The PRESIDING OFFICER. Under the previous order, the motion to proceed to the motion to reconsider the vote by which cloture was not invoked on S. 3414, the Cybersecurity Act of 2012, is agreed to, the motion to reconsider is agreed to, and there is up to 60 minutes of debate equally divided between the two leaders or their designees.

The Senator from Connecticut is recognized.

Mr. LIEBERMAN. Madam President, I want to begin by thanking the majority leader, Senator REID, for being as steadfast as he has been in pursuit of a law that will protect America from what I think most security experts would say today, surprisingly, is the most serious threat to our security and to our economy, which is from cyber attack and cyber theft.

The majority leader, with the authority he has over our schedule, has now pulled up the Cybersecurity Act of 2012, S. 3414, for reconsideration; that is

to say, to reconsider the cloture vote that was held in August and failed to get 60 votes, much to my disappointment. I am very grateful that Senator REID now gives the Senate a second chance to do something to protect the American people from cyber attack and cyber theft.

If you look at what has happened since the cloture vote on the Cybersecurity Act failed back in August, I think you will see how urgently we need to seize this opportunity to at least vote to proceed to the Cybersecurity Act. Senator REID has made clear that he would allow a finite number of amendments—finite because, after all, we are in a postelection so-called lame-duck session. The amendments can't go on forever. But a finite list would allow there to be a discussion and vote on the major concerns people still seem to have with the compromised bipartisan Cybersecurity Act of 2012.

I appeal to my colleagues: Don't be recorded as no. Say yes to at least allowing a discussion of cybersecurity legislation here, offer some amendments, and then, of course, understand that we are not a unicameral legislature, to say the obvious. If—as I hope—we can pass cyber security legislation here, it has to go to conference with the House that I would say has—describing it diplomatically—a different position than as reflected in the Cybersecurity Act of 2012 that emerged in part from the Homeland Security Committee; which is why I have the honor of managing this debate, brought out with the strong support from my ranking member and dear friend Senator COLLINS of Maine, and then working together with Senator FEINSTEIN, the chair of the Senate Intelligence Committee, Senator ROCKEFELLER, the chair of the Commerce Committee, and Senator CARPER, who has had a real interest in cyber security and is a leader on the Homeland Security Committee. We bring this legislation forward.

We are being given a second chance to raise our defenses against rival nations, enemy nations, industrial spies, cyber terrorists, organized anti-American nonstate actors, and international organized criminal gangs who are constantly probing our computer networks for weaknesses that they can exploit to steal industrial secrets, to take some of the best results of American innovation and entrepreneurship overseas and, with it, the jobs that come with those secrets. And, of course, to sabotage critical infrastructure—powerplants, financial systems, telecommunications systems, water systems, and so on and so on—which are the systems that we depend on in our society for our quality of life, for our freedom of expression, so many of them owned by the private sector and managed and controlled now, operated, by cyber systems over the Internet and, therefore, subject to cyber attacks.

That is what this bill is about, creating standards for public-private cooperation to raise our defenses against cyber attack and cyber theft. Everybody you talk to in the public or private sector says today that we are vulnerable to attack. This bill only relates to the most critical cyber infrastructure whose compromise, whose attack, whose disabling would result in mass casualties, catastrophic economic loss, and assaults on our national security.

So let me come back to what I said. The best arguments for this bill and for voting on the motion to proceed and going to the bill are not the arguments, frankly, that I will make on behalf of the bill but the facts that have occurred and the limited amount of time since August when this initial vote to proceed to the Cybersecurity Act occurred.

On August 15, just 2 weeks after the last cloture vote, a computer virus called Shamoon erased the hard drives of 30,000 computers owned and operated by Saudi Aramco, one of the world's largest energy companies. What happened as a result of the erasing of those hard drives, the data files were replaced with images of burning American flags. It is pretty clear who carried out this attack. The computers were rendered useless and had to be replaced and restored. Some cyber experts that I trust say this was the most destructive cyber attack against a private company in history. A similar attack was carried out on the Qatari natural gas company called RasGas. Remember the burning American flags? Iran is suspected as the attacker in both instances.

Thanks to quick work, really extraordinary work by Aramco and many of the world's leading cyber security technologists and experts, the damage to Saudi Aramco was contained. But this attack could have thrown global oil markets into chaos and a lot of economies—including ours—into greater stress than we are already in if orders couldn't be filled or shipments made.

That was August, 2 weeks after the last cloture vote on the cyber security bill. Then in September, the consumer Web banking sites of some great American financial institutions—Bank of America, JPMorgan Chase, Wells Fargo, PNC Bank, and some others—came under the largest sustained denial of service attack in history. As I am sure most of my colleagues know, this is when the Web sites are essentially overloaded, they are flooded, to make it impossible for them to stay up and provide the service they normally do. These attacks went on in different waves for weeks, knocking many of these sites that are very important to commercial life in our country offline or slowing them to a crawl. Just take a look at how much commerce is now conducted over the Internet and I think you can see the potential catastrophe here. These kinds of attacks really could bring our banking system and the economy to its knees. Again, some intelligence officials that I respect suspect that Iran or its agents launched these attacks against the American banks.

Defense Secretary Panetta warned in a recent speech that these and other cyber attacks show that we are approaching a cyber Pearl Harbor where:

> An aggressor nation or extremist group could use these kinds of cybertools to gain control of critical switches . . . [and] derail passenger trains, or even more dangerous, trains loaded with lethal chemicals.
>
> They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country.

That is not science fiction. That is not an alarmist. That is the Secretary of Defense of the United States, Leon Panetta, issuing a warning based on what anybody who works in this field knows is reality.

In recent weeks, we have watched one section of our country—in this case the Northeast, including my own State of Connecticut—hit by Hurricane Sandy and then a follow-on northeaster storm, losing power. Some parts of New York and certainly New Jersey were hit harder than Connecticut, but we were hit pretty hard ourselves. Some still are without power, and this is the third week since the hurricane. This is exactly the kind of dislocation and suffering that would occur if an enemy cyber attacked America's electric power system. It is why we need to at least vote to take this bill up now with a sense of urgency in this session. Time is not on our side.

The elections are over. The American people through their votes have told us in a clear and certain voice that they want us to work together to solve the many challenges our Nation confronts. I know we are focused on avoiding going over the fiscal cliff and the challenge to Congress is, Can we solve our fiscal problems? Can we come to a bipartisan compromise before we go over the cliff?

In this case of cyber security and cyber vulnerability, the challenge before us is, Can we come to a bipartisan agreement compromise—and we think we have in the bill before us—and create and improve our defenses before a catastrophic cyber attack occurs, as it surely will, and then we come rushing back to raise our defenses, as we did after 9/11, after we have suffered an attack?

Mr. WHITEHOUSE. Mr. President, will the Senator yield for a question?

Mr. LIEBERMAN. I will.

Mr. WHITEHOUSE. I want to ask the distinguished chairman, who referenced the important word, ''compromise,'' if he has spoken about the extent to which this bill reflects not only the original bipartisan compromise between himself and his ranking member, Senator SUSAN COLLINS of Maine, but then a second compromise done to reach further to our Republican colleagues that is actually already embedded in this bill. I think it is important for the people who are watching and listening to us to recognize that not only was this an original

bipartisan bill that was the product of bipartisan compromise and discussion, but then a further unilateral step was taken by the distinguished chairman to move even more toward Republican colleagues. So it is not only a compromise but double compromise that is on the Senate floor right now.

Mr. LIEBERMAN. I thank my friend from Rhode Island. I thank my friend for his interest in the area of cyber security and for his leadership. I have not talked about that yet—and I will right now—which is to say, following the advice of most of the experts of both political administrations and experts outside, one of the centerpieces of our original bill was to create a public-private process—government and people who live in these sectors of our economy—to draft best practices, not to have them imposed by the Government, and then to make it mandatory within a set period of time, and that these practices, these standards, would be general principles, not all do's and don'ts, to leave room for the private sector to come up with the best way they thought they could meet those standards.

Opponents, particularly the business community, and some of our friends on the other side, have said to us that they fear that would be more regulation of business. Senator COLLINS, my ranking member and dear friend, is a leading advocate of regulation reform and lighter regulation on business. But she said over and over with such credibility and force: This is not regulation of business; this is protection of our homeland security, of our economy. You reform regulation when the regulations seem to be too much and get in the way of economic growth. We have a threat that is today stealing billions of dollars of American innovation, taking jobs elsewhere in the world.

OK, we had it mandatory, but it was clear we were not going to get to 60 votes. I have said over and over, one of the problems we have in Congress now is people seem to say if they do not get 100 percent of what they want, they are not going to vote for a bill. So I had to listen to my own words because if they wait for 100 percent of what they want on a bill, everybody is going to end up with zero percent. We might as well try to get done what we agree on. So we took a big step, which was to make those mandatory standards voluntary.

Then we threw in an incentive, which is a lot—partial liability, immunity from liability in the case of a cyber attack—as an encouragement for those companies that voluntarily opt into the standards that the voluntary process would set up that gets some immunity from liability for prosecution.

Incidentally, President Obama has made very clear, first, that he totally gets the seriousness of this challenge to our security, this cyber challenge to our security and our prosperity. He has supported this legislation, but he has gone one step further now and said if we fail to pass legislation, he will issue an Executive order that does as much as an Executive order can do to protect America better from cyber attack and cyber theft.

The President does have the authority to issue an Executive order that will establish standards for cyber security for all 18 critical infrastructure sectors under existing law and require those sectors to be implemented in certain areas where the regulators have the power to mandate such observance of the standards. A draft of such Presidential order is now being circulated, but the President does not have the power under existing law to offer a lot of the benefits that our bill would give private sector owners of critical infrastructure.

For one thing the President does not have the ability to offer the private sector owners the liability protection I have just described. In addition, needed changes to law that permit private companies to share cyber security threat information among themselves and with the government will go unmade. So both sides in this debate have acknowledged that this is a critical piece in any bill. But it cannot be implemented by executive action. We are the lawmakers. We have the ability to protect our country better than the President does by Executive order. I have appealed to the President that if we are not able to act here that he should issue this Executive order. I am very encouraged by the work done on it, and I am confident that if we fail to act the President will act. I think he has a responsibility to act because if we fail to act we are leaving the American people extremely vulnerable to a major cyber attack. Therefore, although the legislation is preferable, an Executive order will certainly give the American people protection.

I have more to say, but I note the presence on the floor of my colleague and partner in this pursuit, the chair of the Senate Intelligence Committee, Senator FEINSTEIN. If she would like to speak, I will yield the floor to her.

Mrs. FEINSTEIN. I would, and I thank my colleague.

The PRESIDING OFFICER. The Senator from California is recognized.

Mrs. FEINSTEIN. Madam President, if I may, I want to compliment Senator LIEBERMAN on his steadfast determination to get this bill passed. I think he and his ranking member, Senator COLLINS, have done a very fine job. I think it is important for everyone to know about those hours when we sat down with other Members trying to negotiate something people might agree to on this cyber bill. Unfortunately, we could not.

I am very worried. I am very worried there will be a major cyber attack on this Nation. I do not say that without intelligence to back it up. On the Intelligence Committee, we receive regular warnings from the Intelligence Community that tell us cyber attacks are increasing in number, sophistication, and damage.

Unfortunately, despite significant changes made to the Cybersecurity Act that Senator LIEBERMAN, Senator COLLINS, Senator ROCKEFELLER and I agreed to in July and August, many on the other side of the aisle filibustered the bill. Since that time we have learned of additional major cyber attacks.

In October and September of this year, at least nine major U.S. banks were hit by a series of attacks that blocked their customers from accessing their banking information or making online transactions. This list of victims includes the country's largest, most sophisticated financial institutions: the Bank of America, JPMorgan Chase, Citigroup, the U.S. Bank, Wells Fargo, PNC, Capital One, BB&T Corporation, and HSBC—all cyber attacked.

These attacks systematically hit banks for 5 weeks. They disrupted traffic at each bank for a day or two before moving on to the next victim. It was a well planned and coordinated cyber attack from bank to bank to bank to bank. It disrupted the banking system, but it did not destroy it. But that doesn't mean the attackers do not have the ability to destroy it. This is a real wake-up call, and I think we ignore it at our own peril.

I have come to believe it is negligent to fail to pass a bill with the warnings that are out there today. I remember, I was on the Intelligence Committee when the CIA Director, then-Director Tenet, came before the committee in the middle of the summer in 2001 and said to us: We anticipate an attack. We don't know where. We don't know when. That attack came, and it was 9/11. Today there is the same anticipation of a big attack, a big cyber attack. And we need to put in place the legal procedures to prevent that.

Let me mention other recent cyber attacks. In August, a foreign country or organization used computer code to destroy 30,000 computers at the world's largest energy company, that is Saudi Aramco, and that is Saudi Arabia's state-owned oil company. How is this done? According to the New York Times, the cyber attackers ''unleashed a computer virus to initiate what is regarded as among the most destructive acts of computer sabotage on a company to date. The virus erased data on three-quarters of Aramco's corporate PCs—documents, spreadsheets, e-mails, files—replacing all of it with an image of a burning American flag.''

If anything is a harbinger of things to come, that is clear. Why would one put their signature on a major cyber attack by showing burning American flags unless they had some additional intent against the U.S.? We cannot underestimate the threat. To do so is sheer negligence on the part of this body.

In the 5 months from October 2011 through February 2012, over 50,000 cyber attacks were reported on private and government networks with 86 of

those attacks taking place on critical infrastructure networks. So we have 86 attacks on critical infrastructure networks.

Keep in mind these 50,000 incidents were only the ones reported to the Department of Homeland Security. So they represent but a small fraction of cyber attacks carried out against the United States. This year, 2012, Nissan, MasterCard, and Visa joined the ranks of other major companies already hacked—Sony, Citi, Lockheed Martin, Northrop Grumman, Google, Booze Allen Hamilton, RSA, L–3, and the U.S. Chamber of Commerce as victims of hacking last year.

We also know that last year for at least 6 months, 48 companies in the chemical, defense, and other industries were penetrated by a hacker looking to steal intellectual property. The cyber security company Symantec has attributed some of these attacks to computers in Hebei, China.

Here is the point. We know we are being attacked by other countries. I hear it in the Intelligence Committee. It is classified so I cannot go into it here. But suffice it to say that we know it is happening. Things are only going to get worse, as Secretary Panetta said in a recent major address in New York. Let me just read one section of his speech:

> The collective result of these kinds of attacks could be a cyber Pearl Harbor, an attack that would cause physical destruction and loss of life. In fact it would paralyze and shock the nation and create a new, profound sense of vulnerability.

Members of the Senate, we are warned. We are warned clearly, we are warned directly, and we are warned by the Head of Cyber Command, General Alexander, as well as the Secretary of Defense. Yet we do nothing.

I strongly believe we need to pass this bill. Then it will go to the House. And then there will be a conference. Along the way, there will have to be some accommodations made. But, there is no reason for this Senate, knowing what we know, not to pass this bill.

We also know the President would sign this bill, and we know the President would not sign the House bill as is. So we have an opportunity by moving forward with this bill.

I want to remind my colleagues of efforts made to negotiate an agreement on this bill. Before the bill came to the floor in July, and while the Senate was considering it, there were numerous meetings every day by a dozen or more Senators. The authors of the bill met with Senators McCain, Chambliss, Hutchison, the sponsors of the SECURE IT Act, as well as Senators Kyl and Whitehouse, and a group they convened. We had multiple meetings with the U.S. Chamber of Commerce. The Chamber's largest concern with Title VII on information sharing was over the liability protections in our bill—which is what the Intelligence Committee staff worked on and prepared.

I asked the Chamber where they thought our language was deficient. I asked them if they could improve on the immunity provisions, to please send us bill language. Did they? No. They did not. I think that is some testimony that is worth thinking about.

Over the summer, the majority leader offered to vote on a set list of amendments. He asked if the minority could put together the 10 votes it wanted, and as long as they were relevant and germane to the bill, we would consider them. No list was provided. So we voted, and by a vote of 52 to 46, cloture was not invoked.

Again, after the vote, the staff from both sides of the Homeland Security Committee, the Commerce Committee, and the Intelligence Committee held numerous meetings to negotiate a compromise. The effort did not succeed. So if we are to address the major problem of cyber attacks and potential cyber warfare, we have no option but to bring the Lieberman-Collins bill back on the floor.

I know my time is limited here today. And I know the Nation's cyber laws are woefully out of date. Let me touch on one more thing regarding the information sharing part of the bill. I received a call from a CEO of a high-tech company about the homeland security portal or exchange, as we call it in the bill. That CEO said, We would like our information to go directly into the Department of Defense. Let me note that would create a big problem. It created a problem with a number of U.S. Senators who are concerned about the military getting this kind of cyber information. And it created a big concern with the privacy organizations throughout our country. So it was changed so that the portal would be run most likely by Homeland Security. But here is the point I wish to make. The transfer of cyber information is with the click of a mouse. It moves instantaneously, so that as information——

The PRESIDING OFFICER (Mr. CASEY). The time of the Senator has expired.

Mrs. FEINSTEIN. I ask unanimous consent for 1 minute to conclude.

The PRESIDING OFFICER. Is there objection? Without objection, it is so ordered.

Mrs. FEINSTEIN. So as information comes in, it goes instantaneously into the correct area. The CEO who called me said, I didn't know that. Thank you. I have no problem with that.

So I would ask my colleagues who have voted against this bill to reconsider. We are never going to do the perfect bill. The bills are going to have to be changed and amended as time goes on. But I think passing a bill is important. I think to leave this country vulnerable, not to pass a bill because somebody doesn't like this part or that part, is negligent, it is irresponsible, and God forbid if we have that major cyber Pearl Harbor that Secretary Panetta referred to in his speech. I urge my colleagues to pass this bill.

I thank the Chair for the extra time, yield the floor and ask that my remaining remarks be printed in the RECORD.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

Let me describe what the information sharing title does specifically.

First, title VII explicitly authorizes companies to search for cybersecurity threats on their own networks and to take appropriate actions to defend their networks against these threats.

Many companies monitor and defend their own networks today, in order to protect themselves and their customers.

But we have heard from numerous companies that the law in this area is unclear, and that sometimes it is less risky, from a liability perspective, to just hope attacks don't happen than to take additional steps to defend themselves.

So this bill will make the law crystal clear by giving companies explicit authority to monitor and defend their own networks.

Second, the bill clearly authorizes private companies to share cyber threat information with each other.

There have been concerns that antitrust laws or other statutes prevent companies from cooperating on cyber defense. This bill, section 702, clearly says: ''notwithstanding any other provision of law, any private entity may disclose lawfully obtained cybersecurity threat indicators to any other private entity in accordance with this section.''

Third, the bill authorizes the government—which will largely mean, in practice, the intelligence community—to share classified information about cyber threats with appropriately cleared organizations, such as companies, outside of the government.

Today, only government employees and contractors are eligible to receive security clearances and therefore gain access to national secrets. To put it another way, those with a valid ''need to know'' national security secrets are usually within the government or working for the government.

That isn't true for cyber security. The companies that underpin our Nation's economy and way of life have a ''need to know'' about the nature of cyber attacks so they can better secure their systems.

So under this bill, companies able to qualify to receive classified information will be certified and then be able to obtain classified information about what cyber threats to look out for.

Fourth, the bill establishes a system for any private sector entity—whether a power utility, a defense contractor, a telecom company, or others—to share cyber threat information with the government.

This is the piece that General Alexander—the Director of the National Security Agency and the Commander of U.S. Cyber Command—says is absolutely necessary for the protection of the United States.

Here is how the provision works:

The Secretary of Homeland Security, in consultation with the Attorney General, the Secretary of Defense, and the Director of National Intelligence, would designate a federal cybersecurity exchange. This would be an office or center that already exists, and already shares and receives cyber threat information.

Private companies would share cyber threat information with the exchange directly. The exchange must be a civilian entity; I expect it would be within the Department of Homeland Security.

Let me stop there. Why not have this portal or exchange be in the military or the NSA? There are two reasons:

First, we are talking here about the protection of the government's network—the dot.gov network—and the computer systems outside of the government. We are not talking about protecting the dot.mil network and the Department of Defense, and we are not talking about actions that the military takes overseas. Protection of the private sector—of the electrical grid or Wall Street—is simply not the military's or NSA's responsibility.

Second, there is, for good reason, major concern among privacy advocates not to have private sector information, which could include Americans' banking records, or email traffic, or health care records, being shared by companies with the military or intelligence community.

In drafting this bill, we heard from several Senators for whom having a military exchange was a complete non-starter. We worked with Senators Durbin, Franken, Coons, Akaka, Blumenthal, and Sanders, and others to craft this language putting a civilian entity in the lead.

General Keith Alexander, the Director of the National Security Agency, also supports this model. He wrote, in his July 31 letter to Senator Reid: ''The American people must have confidence that threat information is being shared appropriately and in the most transparent way possible. That is why I support information to be shared through a civilian entity, with real-time, rule-based sharing of cyber security threat indicators with all relevant Federal partners.'' General Alexander is the top military and intelligence official on cyber saying that he supports a civilian exchange.

So we have the Federal exchange. Companies will use the exchange, as a portal and information will be sent automatically and instantaneously to other parts of the government. This is what General Alexander was describing.

This part is critical. We are not talking about information going to an office in the Department of Homeland Security and waiting for someone to look at it and figure out whether to share it and with whom.

This is an automatic, instantaneous process. Information comes in and is automatically shared with other departments and agencies.

The bill requires that procedures be put in place so that information is shared in real-time. This has to be done automatically, so that cyber defense systems can move to identify and disrupt a cyber attack as it is coming over the networks.

I discussed this recently with a CEO of a high-tech company. He was concerned that information wouldn't reach the Department of Defense. I explained that our bill would provide instantaneous sharing to DOD. He said that would satisfy his concerns. So this is a major point.

Having a single focal point is also more efficient for the government. It will help eliminate stovepipes because right now there are dozens of different parts of the government receiving information from the private sector about the cyber threats they are encountering, and no one agency has the responsibility to ensure the information is shared with other parts of the government.

It would also make privacy and civil liberties oversight easier, as I will describe in a moment. Finally, it should save tax payers money, because it is more efficient to manage and oversee the operation of one designated cybersecurity exchange versus a half dozen or more parts of the government.

Now let me describe the liability protections, because that is a critical part of title VII.

Section 706 of the bill provides liability protection for the voluntary sharing of cyber threat information with the federal cybersecurity exchange.

The bill reads: ''no civil or criminal cause of action shall lie or be maintained in any Federal or State court against any entity [meaning a company] acting as authorized by this title, and any such action shall be dismissed promptly for . . . the voluntary disclosure of a lawfully obtained cybersecurity threat indicator to a cybersecurity exchange.''

In other words, a company is immune from lawsuit if it shares cyber threat information with a Federal exchange.

The same immunity applies to:

Companies who monitor their own networks;

Cybersecurity companies who share threat information with their customers;

Companies that share information with a critical infrastructure owner or operator; or

Companies who share threat information with other companies, as long as they also share that information with the Federal cybersecurity exchange within a reasonable time.

If a company shared information in a way other than the five ways I just mentioned, it still receives a legal defense under this bill from suit if the company can make a reasonable good faith showing that the information sharing provisions permitted that sharing.

Further, no civil or criminal cause of action can be brought against a company or an officer, employee, or agency of a company for the reasonable failure to act on information received through the information sharing mechanisms set up by this bill.

Basically, the only way that anyone participating in the information sharing system can be held liable is if they are found to have knowingly violated a provision of the bill or acted in gross negligence.

So there are very strong liability protections in this bill for anyone that shares information about cyber threats—which is completely voluntarily.

In addition to narrowly defining what information can be shared with an exchange, our bill also requires the Federal government to adopt a very robust privacy and civil liberties oversight regime for information shared under this title. There are multiple layers of oversight from different parts of the executive branch, including the Department of Justice and the independent Privacy and Civil Liberties Oversight Board, as well as the Congress.

Consider this: In October, General Alexander—the Director of the NSA—and Anthony Romero, the Executive Director of the ACLU, spoke together on a cybersecurity roundtable at the Woodrow Wilson Center. General Alexander praised title VII's approach to information sharing, and Mr. Romero said ''I think it strikes the right balance.'' It is not often that the Director of the NSA and the Executive Director of the ACLU agree on legislation. If they can, I would hope that the Senate can come together as well.

The time to act is now. The cyber threat we face is real, it is serious, and it is growing. The country is vulnerable, and this legislation is essential. I urge my colleagues to support the motion to proceed and to support the bill.

The PRESIDING OFFICER. The Senator from Georgia.

Mr. CHAMBLISS. Senator GRASSLEY, who is scheduled to speak next, has been kind to give me 45 seconds, so I appreciate that.

In July and August, the cosponsors of both the underlying bill, the Lieberman-Collins bill, and the SECURE IT bill, of which I am a cosponsor, met regularly, and I was hopeful we could resolve the significant differences between these two bills. Unfortunately, we did not reach an agreement, and even though we had been promised an open amendment process on this underlying bill, the majority leader once again filled the tree and filed cloture. Unfortunately, nothing has changed since then, so I am compelled to do the same thing today.

We all understand the serious threat that is facing our country from cyber attacks and intrusions, but that does not mean Congress should just pass any bill. Frankly, the underlying bill is not supported by the business community, for all the right reasons, and they are the ones who are impacted by it. They are the ones who are going to be called on to comply with the mandates and the regulations. Frankly, it is not going to give them the kind of protection they need from cyber attacks.

So I regret to have to stand up today and say that I intend to vote against cloture on this bill, and I yield to Senator GRASSLEY.

The PRESIDING OFFICER. The Senator from Iowa.

Mr. GRASSLEY. Mr. President, we are again discussing the important topic of cybersecurity—a topic we all agree is of the utmost importance and worthy of our attention. Unfortunately, this is like the movie ''Groundhog Day.'' The majority continues to push the same flawed legislation that failed to garner enough votes for consideration just three months ago.

No one disputes the need for Congress to address cybersecurity.

However, Members do disagree with the notion this problem requires legislation that increases the size of the Federal Government bureaucracy and places new burdens and regulation on businesses.

Enhancing cybersecurity is important to our national security. I support efforts to strengthen our Nation against cyber attacks.

However, I take issue with those who have come to the floor and argued that those who don't support this bill are against strengthening our Nation's cybersecurity.

As I said in August, disagreements over how to address policy matters shouldn't devolve into accusations about a Member's willingness to tackle tough issues.

The debate over cybersecurity legislation has turned from a substantive analysis of the merits into a political blame game as to which side supports defending our Nation more.

If we want to tackle big issues such as cybersecurity, we need to rise above disagreements and work in a constructive manner. Disagreements over policy should be openly and freely debated.

Unfortunately, this isn't how the debate on cybersecurity proceeded. Instead, before a real debate began last August, the majority cut it off.

This was contrary to the majority's promise earlier this year of an open

amendment process to address cybersecurity.

Aside from process, I also have significant substantive concerns with the bill. Chief among my concerns with the pending bill is the role played by the Department of Homeland Security. These concerns stem from oversight I have conducted on its implementation of the Chemical Facility Anti-Terrorism Standards, or the CFATS program.

CFATS was the Department's first major foray into regulation of the chemical sector. DHS spent nearly $500 million on the program. Five years later, they have just begun to approve site security plans for the more than 4,000 facilities designated under the rule.

I have continued to conduct oversight on this matter. Despite assurances from DHS that they have fixed all the problems with CFATS, I keep discovering more problems.

On top of this concern, since the last vote in August, the chairman and ranking member of the Senate Permanent Subcommittee on Investigations have released a report criticizing DHS and the fusion centers they operate. The subcommittee report criticized DHS's fusion centers as ''pools of ineptitude, waste, and civil liberties intrusions.''

And that is the evaluation after DHS spent as much as $1.4 billion on this program.

Given these examples, I am baffled why the Senate would take an agency that has proven problems with overseeing critical infrastructure and give them chief responsibility for our country's cybersecurity.

Additionally, I am concerned with provisions that restrict the way information is shared.

The restrictions imposed under title VII of this bill are a step backward from other information-sharing proposals. This includes the bill I have cosponsored, the SECURE IT bill.

The bill before us places DHS in the role of gatekeeper of cyber threat information. The bill calls for DHS to share the information in ''as close to real time as possible'' with other agencies. However, this will create a bottleneck for information coming into the government.

Further, title VII includes restrictions on what types of information can be shared, limiting the use of it for criminal prosecutions except those that cause imminent harm.

This is exactly the type of restriction on information sharing that the 9/11 Commission warned about.

In fact, the 9/11 Commission said, ''the [wall] resulted in far less information sharing and coordination.'' The Commission further added, ''the removal of the wall that existed before 9/11 between intelligence and law enforcement has opened up new opportunities for cooperative action.''

Why would we even consider legislation that could rebuild these walls that threaten our national security?

We haven't had any real debate on these issues. The lack of a real process in the Senate on this current bill amplifies my substantive concerns.

In fact, this is eerily reminiscent of the debate surrounding ObamaCare.

Here we are once again, in a lame duck session the week before Thanksgiving, tackling a serious problem that hasn't been given the benefit of the Senate's full process.

I don't want cybersecurity legislation to become another ObamaCare. If we are serious about our Nation's security, then shouldn't we treat it as such?

Additionally, the staff of the sponsors of the legislation before us continue behind-the-scenes efforts to negotiate changes to the bill we are being asked to vote on. If the bill sponsors are still negotiating changes, why don't we have the benefit of a full and open amendment process to try and fix it before we vote for cloture? It simply doesn't make sense.

Instead, it appears today's vote is about something other than cybersecurity. It is yet another attempt by the majority to paint the minority as obstructing the work of the Senate. Most likely, this vote will be used simply as fuel for the majority's effort to dismantle the filibuster. So much for tackling cybersecurity without putting politics into the mix.

This isn't the way we are supposed to legislate. The people who elected us expect more.

How many Senators are prepared to vote on something this important, without knowing its impact because we haven't followed regular order? Are we to once again pass a bill so that the American public can then read it and find out what is in it?

These are questions that all Senators should consider. And our citizens should know in advance what we are actually considering.

If we are serious about addressing this problem, then let's deal with it appropriately.

Rushing something through that will impact the country in such a massive way isn't the way we should do business.

It is not good for the country and it is not good for this body.

Thank you. I yield the floor.

Ms. MIKULSKI. Mr. President, today I wish to support the Cybersecurity Act of 2012. As a member of the Intelligence Committee, I know that cyber security is the most pressing economic and national security threat facing our country.

There still needs to be a sense of urgency in addressing this issue, and we must pass this legislation. Doing so will allow us to defend our computer networks and critical infrastructure from a hostile, predatory attack. Such an attack is meant to humiliate, intimidate, and cripple us. If we wait until a major attack occurs, we will likely end up over-reacting, over-regulating, and overspending in order to address our weakness.

The threat of a cyber attack is real. Our Nation is already under attack. We are in a cyber war, and cyber attacks are happening every day. Cyber terrorists are working to damage critical infrastructure through efforts to take over the power grid or disrupt our air traffic control systems. Those carrying out these attacks are moving at breakneck speeds to steal state secrets and our Nation's intellectual property. They are stealing financial information and disrupting business operations.

Cyber attacks can disrupt critical infrastructure, wipe out a family's entire life savings, and put human lives at risk. They can take down entire companies by hacking into computer networks where they remain undiscovered for months, even years.

FBI Director Mueller testified before the Senate Intelligence Committee, stating that cyber crime will eventually surpass terrorism as the No. 1 threat to America. The economic losses of cyber crime alone are stunning. A Norton Cybercrime Report valued losses from cyber attacks at $388 billion in 2011.

I have been working on cyber issues since I was elected to the Senate. The National Security Agency—our cyber warriors—are in Maryland. I have been working with the NSA to ensure that signals intelligence is a focus of our national security even before cyber was a method of warfare.

In 2007, Estonia was attacked. Estonia was strengthening its ties to NATO, and Russian hackers swiftly struck back. They waged war on Estonia and threatened its government, rendered Estonia's networks obsolete for days. This attack was designed to intimidate, manipulate, and distort.

The cyber attacks on Estonia raised important questions. Would article 5 of the NATO Charter be invoked? Since the attack was on one member of NATO—was it an attack on all members? How would the U.S. and other allies need respond to future attacks? What would happen if America experienced a similar cyber attack?

As member of the Senate Intelligence Committee, I served on the Cyber Working Group where we developed core findings to guide Congress. The need to get governance right, the need to protect civil liberties, and the need to improve the cyber workforce.

As chair of the Commerce, Justice, Science Appropriations Subcommittee, I fund critical cyber security agencies: the FBI which investigates cyber crime, NIST, which works with the private sector to develop standards for cyber security technology, and NSF, which does research.

As a member of Defense Appropriations Subcommittee, I work to ensure critical funding for Intel and cyber agencies such as the NSA, CIA, and IARPA. These organizations are coming up with the new ideas that will create jobs and keep our country safe.

Funding is critical to build the workforce, provide technology and resources, and to make our cyber security smarter, safer, and more secure.

Yet technology will mean nothing unless we have a trained workforce. In order to fight the cyber security war, we have to maintain our technological development, maintain our qualitative advantage, and have our cyber warriors ready at battle stations. In order to develop our cyber shield, we need to train cyber warriors so they can protect our Nation. I have been working with Maryland colleges and universities to create world-class programs, a national model, and for training our next generation of cyber warriors.

I asked Senator REID to conduct a cyber security exercise, which showed us in real time how the U.S. Government would respond to a predatory cyber attack of great magnitude. I asked for the Senate cyber exercise for three reasons. First, we need a sense of urgency here in the Senate to pass cyber security legislation. Second, we need to put the proper legislative policy in place. Third, I wanted to create a sense of bipartisanship camaraderie.

One example of the impact a cyber attack would have is the power outages caused by our freak storms this summer. We got a glimpse of what an attack on the grid would be like. At least Pepco has the ability to respond and restore and turn the power back on. With an attack on the grid we could lose the power to turn electricity back on because it was shut down by power manipulation. Imagine our largest cities, like New York and Washington, like the Wild West with no power, schools shut down, parents stuck in traffic, public transit crippled, no traffic lights, and 9-1-1 systems failing.

In the financial industry, the FBI currently has 7,600 pending bank robbery cases and over 9,000 pending cyber investigations. According to the FBI, the Bureau is currently investigating over 400 reported cases of corporate account takeovers where cyber criminals have made unauthorized transfers from the bank accounts of U.S. businesses. These cases involve the attempted theft of over $255 million and actual losses of approximately $85 million.

Hackers have repeatedly penetrated the computer network of the company that runs the Nasdaq Stock Market. The New York Stock Exchange has been the target of cyber attacks. In the future, successful attempts to shut down or steal information from our financial exchanges could wreak havoc of untold proportions on our economy.

In the 2010 ''flash crash'', the Dow Jones plunged 1,000 points in matter of minutes when automatic computerized traders shut down. This was the result of turbulent trading, not a cyber attack and the market recovered. But this is a micro-example of what could happen if stock market computers are hacked, infected, or go dark.

In November 2008 the American credit card processor RBS Worldpay was hacked—$9 million was stolen in less than 12 hours. The hackers broke into accounts and changed limits on payroll debit cards employees use to withdraw their salaries from ATMs. The cards were used at over 2,100 ATMs in at least 280 cities around the world, United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan, Canada, stealing over $9 million from unsuspecting employers and employees.

This heist, one of the most sophisticated and organized computer fraud attacks ever conducted proves that you don't need a visa to steal someone's visa card.

From 2008 to 2010, a Slovenian citizen created ''Butterfly Bot'' and sold it to other criminals worldwide. Cyber criminals developed networks of infected computers. The Mariposa variety from Spain was the most notorious and largest. Mariposa infected personal computers, stole credit card and bank account information, launched denial attacks to shut down online services, and spread viruses to disable computers and networks.

Industry experts estimated the Mariposa Botnet may have infected as many as 8 million to 12 million computers. The size and scope of the infection makes it difficult to quantify financial losses but could easily be tens of millions of dollars.

Speaking simply, this bill does two key things from a national security perspective. It helps businesses voluntarily get cyber standards that they can use to protect themselves, and it allows businesses and the government to share information with each other about cyber threats. That is, to help ''.gov'' to protect ''.com.''

In a constitutional manner, these two things are not necessarily connected, but they can be. The reason why these provisions are such an innovation is that despite all the amazing talent and expertise that companies have, many are being attacked and don't know it. And this legislative framework gives the structure to allow for unprecedented ''.com'' and ''.gov'' cooperation.

There are also other several other key components in the bill focusing on research and development, workforce development, and FISMA reform.

Why do we need a bill to make some of these vital partnerships and exchanges happen?

Because, as I have outlined, America is under attack every second of every day. General Alexander, the head of NSA and U.S. Cyber Command, has said that we have witnessed the greatest transfer of wealth in history in the heist that foreign actors have perpetrated on our country. By stealing our secrets, stealing our intellectual property, and stealing our wealth. It is mindboggling. Take just one example. A theft by a foreign actor that took, among other things, key plans for our F–35 fighter. One attack on the Pentagon made off with so many sensitive documents that they would have filled delivery trucks end-to-end stretching from Washington, DC to Baltimore Harbor.

But don't take my word for it that this issue is urgent and that we need to address critical infrastructure. Who else says it is urgent? Experts from both side of the aisle do. Folks like former CIA Director Mike McConnell, DHS head Michael Chertoff, Vice Chairman of the Joint Chiefs of Staff James Cartwright, former cyber czar Richard Clarke, and many others have said we need to address critical infrastructure.

And our top defense and military leaders such as Defense Secretary Leon Panetta, Chairman of the Joint Chiefs of Staff Dempsey, Director of National Intelligence Clapper, and again, GEN Keith Alexander. The threat is here and it is now. And if we do not act, if we let the perfect be the enemy of the good, then this country will be more vulnerable than ever before, and Congress will have done nothing.

This bill is not perfect, but I want to say upfront that Senators LIEBERMAN and COLLINS have heard the critics and tried to incorporate their views. DHS's role has been criticized by many, myself included. I have been skeptical that they could perform some of the duties assigned in this bill.

To be honest, I still am skeptical, although less so than before, but I think this bill takes important steps to diversify the government and private sector actors involved. So we are not just focusing on DHS, but also the right civilian agencies in charge because in the end we cannot have intelligence agencies leading this effort with the private sector. Some would like to see that go further, and that is what the amendment process is there for.

We have had people in the civil liberties community worried about whether this bill could allow intrusions by the government into people's privacy. As a Marylander, this was a tantamount concern for me as well. If we don't protect our civil liberties, then all this added security is for naught because we would have lost what we value most, our freedom.

Again, I think the authors of this bill, especially Senator FEINSTEIN, have made key improvements on issues of law enforcement powers and protecting core privacy concerns. I know not everyone is totally pleased. But I think this bill has made important strides to balance information sharing and privacy.

We all have been concerned that the business community has opposed a lot of key critical infrastructure elements of this bill. They fear strangulation and over-regulation. They fear that they will open themselves up to lawsuits if they participate in the program with the government. These are valid concerns, and I have heard them from Maryland businesses. I think this new bill has made the most strides in trying to accommodate business and

building a voluntary framework to allow businesses to choose protection.

Protection does not come without responsibility for participants, but I think this bill links the need for cyber security with appropriate liability protection and the expertise of our business community in a way that answers a lot of companies' concerns. We cannot eliminate all government involvement in this issue. That won't work. And we will lose key government expertise in DOD, FBI, and elsewhere. But we work to try to minimize it while maintaining government's role in protecting our national security.

I am so proud that the Senate came together in a bipartisan way to draft this legislation. The Senate must pass this legislation now. Working together we can make our Nation safer and stronger and we can show the American people that we can cooperate to get an important job done.

Mr. ROCKEFELLER. Mr. President, for 4 years, we have been pushing the United States Senate to pass a bill to improve our Nation's cybersecurity. During this time, the cybersecurity threat to our country—to our way of life—has only grown. We have now seen cyber attacks against our Nation's pipelines, against our financial industry, and even against nuclear power plants.

The good news is we have not yet suffered a devastating cyber attack. At this point, we are still only talking about the potential impacts. We have not yet suffered an attack that greatly disrupts our financial industry, or an attack that cripples our electric grid. But these potential outcomes are real. And it is imperative that we begin addressing the risks.

Today, we have the opportunity to begin this important work by moving forward with the Cybersecurity Act of 2012. We have the opportunity to show the American people that we can rise above politics to do the job that they expect of us.

National security is one of our most sacred obligations as Members of this body. If a vote on cybersecurity fails today, we will have failed to meet that obligation for the 112th Congress.

I will be the first person to admit that this bill is not perfect. I have been clear that I believe a regulatory approach was the best approach to ensure that our country's most critical infrastructure addresses its cybersecurity vulnerabilities. We moved to a voluntary approach to seek a compromise. Yet it was not enough for some of our colleagues. Frankly, I do not understand why.

I know the Chamber of Commerce decided that it did not like this bill. But sometimes we need to make decisions that the Chamber of Commerce is not happy with. Because it is not the Chamber's job to worry about national security. That is the job of our military. And they have been quite clear about what is needed. They have told us that they need this legislation. They have implored us to act. General Alexander, the Director of the National Security Agency, knows what is at stake. And his warnings have been dire.

He has said: ''The cyber threat facing the Nation is real and demands immediate action.''

He has said: ''the time to act is now.''

General Dempsey, the Chairman of the Joint Chiefs of Staff, wrote me a letter earlier this year about the urgent need for comprehensive cybersecurity legislation. In the letter, he explained that our: ''adversaries will increasingly attempt to hold our Nation's core critical infrastructure at risk.''

He stated that: ''we cannot afford to leave our electricity grid and transportation system vulnerable to attack.''

Both Generals agreed that we must do something and they both pushed the Senate to adopt comprehensive cybersecurity legislation that tracks the specifics of the bill we have been debating. Despite this urgent advice from our nation's top military advisors, that we need to act and that we need to do it now, some Senators suggested in August that we needed more time to debate cybersecurity. I strongly disagreed with this notion. But now we have had another few months to think about this bill. Today, there is simply no more reason for delay.

We passed a Cybersecurity bill out of the Commerce Committee in March 2010. And it passed unanimously. The Homeland Security Committee, led by Senators Lieberman and Collins, passed their cybersecurity bill by a voice vote in June 2010. The bills both went through Committees well over 2 years ago. Since that time, we have had hundreds of meetings with the private sector, interest groups, and national security experts. Senators have received multiple classified briefings about the nature of this threat. Everyone has had plenty of time to think about this issue. And we have made it quite clear that we are looking to compromise on this legislation. But to compromise you need a partner. I am hoping that our Republican colleagues are now willing to be our partners on this legislation.

I hope that my colleagues will reconsider the path we are on. At some point, if we do not do anything, there will be a major cyber attack and it will do great damage to the United States. After it is over, the American people will ask, just as they asked after 9/11, what could we have done to stop this?

If we do not pass this legislation, they will learn about days like this one and their disappointment in us and the United States Senate will grow. And we will deserve their disappointment. Because we have had the opportunity to act and we have failed.

The PRESIDING OFFICER. The Senator from Texas.

Mrs. HUTCHISON. How much time is remaining on our side?

The PRESIDING OFFICER. There is 20 minutes remaining.

Mrs. HUTCHISON. Thank you. Are there other speakers on our side? Let me ask the Chair to notify me when there is 10 minutes left in case Senator COLLINS comes or someone else. So I would like to have up to 10 minutes and be notified.

Mr. President, I rise to speak against revoting this cloture motion, and the main reason is that we are not going to be allowed to have amendments. That is unacceptable because although we have worked diligently with the sponsors of the cyber security bill on the floor, a number of the ranking members of the relevant committees that have jurisdiction over cyber security have an alternative bill, the SECURE IT Act, that we would like to be able to put forward as an alternative or have an amendment process that would allow our approach to have a chance to prevail anyway.

Now, we are aware that the President is signaling his intention to issue an Executive Order, but an Executive Order is not sufficient to really give the encouragement and the protection to the companies to allow them to share information with other companies that might have the same types of threats in the same industry area or with the Federal Government. I am sorry we are not going to be able to have amendments that would allow us to perfect this bill.

Let me say that the proponents of S. 3414 acknowledge that it is important to have a collaborative effort between the businesses that run almost 90 percent of our Nation's critical infrastructure and the Federal Government. We agree with that, which is why we have worked with the companies that run the private networks to fashion a bill that would give them immunity if they share information and give them the direct sharing capabilities to go directly to the defense agencies because we believe the agencies that work with the communications and the military industrial base companies would have more of an understanding of the needs and what can be done to employ countermeasures in a direct way. The bill that is on the floor, however, requires everything to go through the Homeland Security Department, and those of us who are supporting SECURE IT believe there should be the ability to direction share information with other agencies including the defense agencies.

The sponsors of our bill are the ranking members of eight committees and subcommittees that have jurisdiction in this area: Senators MCCAIN, CHAMBLISS, GRASSLEY, MURKOWSKI, COATS, BURR, JOHNSON, myself and Minority Leader MCCONNELL. We believe the consensus items in our bill are preferable to the bill that is before us that we are not going to be allowed to amend.

SECURE IT offers a balanced approach that will significantly advance cyber security in both the public and private sectors—first, to facilitate

sharing of cyber threat information between the private sector and government, allowing the information to go to the defense agencies where the response can be direct, not filtered through Homeland Security. Secondly, it gives immunity from liability for sharing among the industries that might be affected as well as the defensive actions that are taken. This is essential because you even need antitrust protection if you are going to share vital information on this issue so that you are not going to get sued for collaborating with a competitor. It is in our country's interest, and I think our private sector companies want the ability to help secure all of our networks because we know this is a real threat.

Secure IT has the overwhelming support of the network operators that are trying to gear up to defend against cyber threats. Because it will help their members protect their networks, we have the endorsement of the U.S. Chamber of Commerce.

Mr. President, I ask unanimous consent to have printed in the RECORD a letter from the U.S. Chamber of Commerce dated November 14 of this year.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA,
Washington, DC, November 14, 2012.

TO THE MEMBERS OF THE UNITED STATES SENATE: The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than three million businesses and organizations of every size, sector, and region, continues to have serious concerns with S. 3414, the ''Cybersecurity Act of 2012,'' including the related manager's amendment, which was debated in the Senate before the August recess.

The Chamber believes that Congress should approve a workable cybersecurity bill focused on information sharing. The waning days of a lame-duck session are hardly the appropriate place to address the fundamental flaws in a bill that remain unresolved since it was last on the Senate floor. The underlying issues are simply too crucial to our economy for treatment in a rushed legislative product.

First, there is a healthy and robust disagreement about the proper role of government in regulating the business community—given the incredibly dynamic nature of cybersecurity risks—that is far from resolved. Title I of S. 3414 would create a National Cybersecurity Council that would give federal departments and agencies overwhelming authority over what actions businesses could take to protect their computers and information systems.

Critical infrastructure owners and operators are concerned that core threats to enterprise cybersecurity—including nation states or their proxies, organized criminals, and other nefarious actors—could go unchallenged because they would be compelled to redirect resources toward meeting government mandates. Indeed, any cybersecurity program must afford businesses maximum input and flexibility with respect to implementing best cybersecurity practices.

In addition, insufficient attention has been paid to the likelihood of creating a well-intended program that, in practice, becomes slow, bureaucratic, and costly. An ineffective program would tie businesses in red tape but would do little to deter bad actors. Businesses do not have unlimited capital and human talent to devote to regulatory regimes that are inadequately managed or out of date as soon as they are written.

Second, the Chamber agrees with most lawmakers that federal legislation is needed to cause a sea change in the current information-sharing practices between the public and private sectors. Title VII of the bill would actually impede the sharing of information between business and government. The bill's framework and strict definition of cyber threat information would erect, not bring down, barriers to productive information sharing.

Third, the liability ''protection'' provisions throughout the bill need to be further clarified and strengthened. Private-sector entities should be fully protected against liability if they ''voluntarily'' adopt a federally directed cybersecurity program and suffer a cyber incident. Strong liability protections are essential to spur businesses to share threat data with their peers and government partners.

Fourth, the ''Marketplace Information'' provision of S. 3414 seems intended to compel businesses that suffer from a cybersecurity event to publicly disclose the occurrence. This section of the bill would essentially ''name-and-shame'' companies and could compromise their security. The Chamber strongly rejects disclosing businesses' sensitive security information publicly, and draws your attention to a June 2011 letter from the Securities and Exchange Commission to the Senate where the agency stated that investors have not asked for more disclosure in this area.

Finally, the bill has not been scored, making the cost of the bill unknown to lawmakers and to the public.

These are some of the Chamber's high-level concerns with S. 3414. The Chamber and our members have invested considerable time and energy working with lawmakers to develop smart and effective cybersecurity legislation. The business community is fully prepared to work with Congress and the Administration to advance efforts that would truly help business owners and operators counter advanced and increasingly sophisticated cyber threats.

Cybersecurity is a pressing issue that the Chamber remains committed to addressing in a constructive way. Moving a large, problematic bill within a short legislative timeframe would not lay the necessary groundwork to help businesses deflect or defeat novel and highly adaptive cyber threats. Any new legislative program must foster timely and actionable information, be dynamic in its execution, and promote innovation in order to increase collective cybersecurity and allow electronic commerce to grow.

The Chamber recognizes the leadership of the sponsors and cosponsors of the bill on cybersecurity. We appreciate the degree to which they have listened to the concerns of the Chamber and the broader business community, and have sought to address them in whole or in part. This legislation came directly to the floor for consideration without proceeding through regular order. Legislative hearings and a committee mark-up of the bill would have properly allowed Senators who have concerns with the bill to question experts and offer amendments in order to improve the bill before a Senate floor debate.

The Chamber appreciates the steps that the Administration has taken to engage the Chamber on cybersecurity. Despite all this engagement, and despite the best intentions of the sponsors of S. 3414, it would be ill-advised to craft a cybersecurity bill on the Senate floor during a lame-duck session.

The Chamber strongly opposes S. 3414, the ''Cybersecurity Act of 2012,'' and may consider including votes on, or in relation to S. 3414 in our annual How They Voted scorecard.

Sincerely,

R. BRUCE JOSTEN,
Executive Vice President, Government Affairs.

Mrs. HUTCHISON. We also have the endorsement of the National Association of Manufacturers, the American Fuel & Petrochemical Manufacturers, the American Petroleum Institute, US Telecom, the National Retail Federation, Financial Services Roundtable, the Internet Security Alliance, and CTIA The Wireless Association.

We can come together to pass the areas of SECURE IT that would allow better cooperation and also an information sharing relationship that they understand and know will help them defend against the cyber attacks. We believe SECURE IT is a superior bill, and we would like the ability to amend the bill that is on the floor to perfect it so we could send a bill to the House.

If we are not able to get this bill this year, certainly I hope it will be started again with all of the relevant committees doing the markups, doing the discussion that is required for a bill of this magnitude. Many of the committees did not have markups. They did not have input into the bill. The committee process does work when we are able to use it, and I hope we will be able to go back to the drawing board, or if the majority would allow amendments down the road, if we have the time later this year, we would love to continue working with the sponsors of the legislation to see if we could come up with the amendments to which everyone could agree.

It has been a tough road. We have all tried hard. I think the sponsors of the bill are sincere in wanting to improve the systems. The ranking members who have cosponsored SECURE IT, who also have jurisdiction of this area, also are sincere. I hope we can come together, hopefully later this year, but if not, certainly in the new year, with the new session, let's start from the beginning and go through all the committees of jurisdiction so there can be a real consensus and a give-and-take.

Mr. President, I thank you and yield the floor.

The PRESIDING OFFICER. The Senator from Connecticut.

Mr. LIEBERMAN. Mr. President, I ask unanimous consent to speak for up to 1 minute and not have the time taken out of the Republican side.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

Mr. LIEBERMAN. Mr. President, I want to respond to the concern of my friend from Texas that if cloture is granted on this motion, there will not be an opportunity to amend the bill. I understand why she is saying that, but I do want to say that Senator REID has made it clear—I think twice today—that if cloture is granted, he is open

to—he will allow amendments. He said he cannot allow endless amendments because we are in a lameduck session with limited time but that he will allow a finite number of amendments, if you will, on both sides.

So I want to assure my colleagues and appeal to my colleagues to vote to at least consider this measure. I mean, our cyber enemies are at the gates. In fact, they have already broken through the gates. The least we can do is debate and vote on amendments to determine how we can strengthen our cyber defense.

I thank my colleagues and yield the floor.

The PRESIDING OFFICER. The Senator from Maine.

Ms. COLLINS. Mr. President, first, let me thank the Senator from Texas for reserving some time for me while I was at a briefing and on my way to the floor. I will attempt to be very quick because I know our colleagues are eager to vote on this important issue. And, Mr. President, that is my point. This is a critically important issue. How many more warnings do we need to hear from the experts that we are extremely vulnerable to a cyber security attack? Cyber attacks are happening every day.

Just recently there was an attack on several of our financial institutions. According to press reports, it was launched by Iranian sources. We know that Iran, Russia, and China are extremely active in probing our cyber systems, including those that control our critical infrastructure—not only our financial systems, our transportation systems, our water treatment plants, but also our electric grid.

Recently we have seen what Hurricane Sandy, the superstorm, has done to States—so many States—destroying lives and property and leaving people without power for days on end. Well, multiply that many times. If it were a deliberate cyber attack that knocked out the electric grid along the entire east coast, that is what we are talking about. That is the kind of risk that calls us to act.

We have heard from the experts over and over again that this vulnerability is huge and escalating. We know that the number of cyber attacks that have been reported to the Department of Homeland Security has increased by 200 percent in just the last year. And those are just the attacks that have been reported. That is just the tip of the iceberg. Undoubtedly, there are many more on our critical infrastructure that have not been reported. We know there have been attempts to probe the security of the computer systems that run some of our natural gas pipelines.

This problem is very real, and it is not only a threat to our national and homeland security, it is also a threat to the economic prosperity of this country. How many more thefts of research and development, of intellectual property of businesses right here in our country that are providing good jobs for Americans do we need to endure before we act to secure our cyber systems?

I have worked on the cyber security bill for years with my friend, colleague, and chairman, JOE LIEBERMAN. We have held countless hearings. We have marked up a previous bill. It is so ironic that we are being criticized for not doing yet another markup on this bill when all of the changes reflect our attempts to address the criticisms of the opponents of this bill. We made a huge change by making this bill voluntary rather than mandatory and by providing incentives such as liability protections for businesses that voluntarily agree to adopt cyber standards. We have created a system where there would be a cooperative process between the public and the private sectors to share information and to develop the best practices so that information can be shared.

In all the time I have worked on homeland security issues, I cannot think of another threat where our vulnerability is greater and where we have failed to act and have done less.

This is not a Republican or a Democratic or an Independent issue. The experts, regardless of their political leanings, from the Bush administration to the current administration have urged us to act, have pleaded with us to act.

General Alexander, the nonpartisan general who is the head of Cyber Command and the head of the National Security Agency, has urged this Congress over and over again to give this administration, to give our country the tools it needs to protect critical infrastructure and to help safeguard our economic edge.

I urge our colleagues to listen to the wisdom of former Homeland Security Secretary Michael Chertoff and former NSA chief GEN Michael Hayden from the previous administration, from President Bush's administration. They wrote the following:

> We carry the burden of knowing that 9/11 might have been averted with the intelligence that existed at the time. We do not want to be in the same position again when ''cyber 9/11'' hits—it is not a question of ''whether'' this will happen; it is a question of ''when.''

This time all the dots have been connected. This time we know cyber attacks are occurring each and every day. This time the warnings are loud and clear. How can we ignore these dire warnings? How? How can we fail to act on the cyber security bill, especially since the majority leader has indicated he is willing to allow for amendments, as he should, to make this process fair. Germane amendments would be allowed.

I urge our colleagues to heed the warnings from the experts and to vote for cloture on the cyber security bill so we can proceed to its consideration. I do not want to be here 1 year from now saying, why did we not act? Why did we not listen to the cyber experts from the Bush administration, from the Obama administration, from GEN Keith Alexander, the premier expert in our government.

I yield the floor.

The PRESIDING OFFICER. The Senator from Delaware.

Mr. CARPER. Mr. President, I ask unanimous consent to speak for 1 minute.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. CARPER. Mr. President, this is the first opportunity we will have had since returning from the election to cast a vote on a meaningful piece of legislation. As legislation goes, it is about as meaningful as any we are going to come across for a while.

If we were in the minority and the Republicans were coming to the floor and asking us to support moving to a bill so we could debate it, offer amendments to the bill, I would hope we would do that. For our Republican friends who are fearful they are not going to have a chance to offer these amendments, Senator LIEBERMAN, the chairman, the ranking Republican SUSAN COLLINS and myself, all cosponsors of the bill, say we will work very hard to make sure any amendments that are relevant and germane to the bill can be offered, can be debated.

We worked a similar process with the postal bill. We ended up having 50 or 60 amendments. They were not all relevant or germane. At the end, we had a lot of amendments and the chance for everyone to be heard. Some of those amendments were not relevant or germane. As long as amendments are relevant and germane to this underlying legislation on cyber security, we will work very hard to make sure they have their opportunity to be heard and to vote on their proposals.

The PRESIDING OFFICER. The Senator from Maine.

Ms. COLLINS. Mr. President, although we have different views on this issue, I would yield 1 minute to the Senator from Arizona.

Mr. MCCAIN. Mr. President, I would like to express my appreciation for Senator LIEBERMAN's and Senator COLLINS' hard work. We have had some disagreements. I still believe that if we could have, say, five amendments that would be voted and debated, I think we could move forward with this bill. I truly believe that.

I would like to see, possibly even right after this vote, if we could reach some agreement between the leaders and ourselves that we could say there would be five pending amendments and perhaps we could go ahead and debate and vote on those. I, again, think we have some very significant differences, but the fact that the chairman and the two cochairmen or whatever they call themselves have worked incredibly hard on this issue, they deserve debate. I hope they would understand we are seeking like five amendments.

The PRESIDING OFFICER. The Senator from Connecticut.

Mr. LIEBERMAN. Mr. President, in the remaining time, I appreciate what my friend from Arizona said. I not only join him in that request, but I am confident because I have talked to Senator REID about this—he said that if we invoke cloture tonight, he will allow a finite number of amendments. I do not want to encourage anyone. He said not 15. I took that to be some number less than 15.

I think five amendments is well within the term ''finite.'' So I would ask my colleagues, give it a chance, and let's vote for cloture. I am sure Senator REID will allow five amendments.

CLOTURE MOTION

The PRESIDING OFFICER. The cloture motion having been presented under rule XXII, the Chair directs the clerk to read the motion.

The assistant legislative clerk read as follows:

CLOTURE MOTION

We, the undersigned Senators, in accordance with the provisions of Rule XXII of the Standing Rules of the Senate, hereby move to bring to a close debate on S. 3414, a bill to enhance the security and resiliency of the cyber and communications infrastructure of the United States.

Harry Reid, Joseph I. Lieberman, Barbara A. Mikulski, Thomas R. Carper, Richard J. Durbin, Christopher A. Coons, Mark Udall, Ben Nelson, Jeanne Shaheen, Tom Udall, Daniel K. Inouye, Carl Levin, John D. Rockefeller IV, Charles E. Schumer, Sheldon Whitehouse, John F. Kerry, Michael F. Bennet.

The PRESIDING OFFICER. By unanimous consent, the mandatory quorum call has been waived.

The question is, Is it the sense of the Senate that debate on S. 3414, a bill to enhance the security and resiliency of the cyber and communications infrastructure of the United States, shall be brought to a close?

The yeas and nays are mandatory under the rule.

The clerk will call the roll.

The assistant legislative clerk called the roll.

Mr. DURBIN. I announce that the Senator from Hawaii (Mr. INOUYE), is necessarily absent.

Mr. KYL. The following Senator is necessarily absent: the Senator from Illinois (Mr. KIRK).

The PRESIDING OFFICER (Mr. BENNET). Are there any other Senators in the Chamber desiring to vote?

The yeas and nays resulted—yeas 51, nays 47, as follows:

[Rollcall Vote No. 202 Leg.]

YEAS—51

Akaka	Conrad	Lautenberg
Begich	Coons	Leahy
Bennet	Durbin	Levin
Bingaman	Feinstein	Lieberman
Blumenthal	Franken	Lugar
Boxer	Gillibrand	Manchin
Brown (MA)	Hagan	McCaskill
Brown (OH)	Harkin	Menendez
Cantwell	Johnson (SD)	Mikulski
Cardin	Kerry	Murray
Carper	Klobuchar	Nelson (NE)
Casey	Kohl	Nelson (FL)
Collins	Landrieu	Reed
Reid	Shaheen	Udall (NM)
Rockefeller	Snowe	Warner
Sanders	Stabenow	Webb
Schumer	Udall (CO)	Whitehouse

NAYS—47

Alexander	Graham	Murkowski
Ayotte	Grassley	Paul
Barrasso	Hatch	Portman
Baucus	Heller	Pryor
Blunt	Hoeven	Risch
Boozman	Hutchison	Roberts
Burr	Inhofe	Rubio
Chambliss	Isakson	Sessions
Coats	Johanns	Shelby
Coburn	Johnson (WI)	Tester
Cochran	Kyl	Thune
Corker	Lee	Toomey
Cornyn	McCain	Vitter
Crapo	McConnell	Wicker
DeMint	Merkley	Wyden
Enzi	Moran	

NOT VOTING—2

Inouye	Kirk

The PRESIDING OFFICER. On this vote, the yeas are 51, the nays are 47. Three-fifths of the Senators duly chosen and sworn not having voted in the affirmative, upon reconsideration, the motion is not agreed to.

The majority leader.

ORDER OF BUSINESS

Mr. REID. Mr. President, the bill that was, and is, most important to the intelligence community and to the Pentagon was just killed. I am speaking of the cyber security bill.

I have had a number of people come to me during the day and say: Are you going to allow relevant amendments on this? I said: Sure. They said: How about five? I said: Fine. But whatever we do on this bill, it is not enough for the Chamber of Commerce. It is not enough.

So everyone should understand, cyber security is dead for this Congress. What an unfortunate thing. But that is the way it is.

I filed cloture on the Sportsmen's bill yesterday. Unless we can agree to a limited number of amendments, we will have a cloture vote on the bill early tomorrow morning, probably around 9 o'clock. If we get cloture, there will be a potential 30 hours of debate under the rules, as we all know too well. I have been told someone on the other side also plans to make a Budget Act point of order against the Sportsmen's bill.

We have Members representing the States of New York and New Jersey who are going to be in their States tomorrow because of the tremendous damage caused by Sandy, but they will be back here tomorrow evening and we will have a vote in the morning on cloture on the Sportsmen's bill, and then we could have votes later tomorrow or on Friday.

On DOD authorization—Senator LEVIN is here, Senator MCCAIN was here earlier. I have had conversations with Senator LEVIN. I haven't spoken to Senator MCCAIN this week but have spoken to him previously on a number of occasions. This is a bill we should get done. It is an important piece of legislation. I know we have the Defense appropriations bill at a later time, but this is something we have to do now because it changes policy toward our fighting men and women around the world. It does a lot of good for them. We need to get this bill done, I repeat.

Probably what we are going to do is move to the bill. I don't know why in the world we have to file cloture on a motion to proceed to it. I don't quite understand that. But I haven't understood that about almost 400 times the last few years. So what we are going to do, and everyone should understand—listen to this, everybody—we are going to move to the bill. If we get permission to go to the bill, we will have an open amendment process on this bill. I have been assured by Senator LEVIN and Senator MCCAIN, through Senator LEVIN, that on all these nonrelevant, vexatious amendments they will help us table them or dispose of them in some appropriate manner. And that is how we should legislate around here.

I hope Senator MCCAIN, after speaking to Senator LEVIN, will agree to move forward on this bill. And that is my proposal. I hope it is something that everyone would agree to. We will start legislating on this bill the day we get back after the Thanksgiving recess.

Mr. CARPER. Would the majority leader yield for a question?

Mr. REID. Yes.

Mr. CARPER. I am pleased to hear the leader say he would be most willing to allow the minority to offer five relevant, germane amendments to the cyber security legislation. Literally within the last 30 minutes we have had on the floor both the leader saying this, and I have heard him saying it before, that a limited number of relevant amendments—Senator MCCAIN came to the floor, who, as you know, has not been anxious to support the bipartisan legislation developed by Senators LIEBERMAN and COLLINS and others—but we have had one of the antagonists to that legislation and the majority leader both saying that five relevant and germane amendments would be allowed for the minority to offer, so we could at least take up the bill, debate the bill. At the end of the day, we still need 60 votes to get the bill off the floor.

I have heard so many of my colleagues say it is not a matter of if but it is when, and I don't want us to leave and go home for Thanksgiving with this hanging, if we could actually do something relevant.

Mr. REID. Mr. President, just so everyone listening to my friend understands—and he also has worked so hard on the bill that was just killed—when he says it is not a question of if, it is when, he is not talking about passing this bill, he is talking about a cyber attack, a gargantuan cyber attack on our country.

Here we are in this beautiful Capitol building today, and all around America we have government officials and private sector officials who are trying to thwart the people trying to destroy businesses and parts of our country's infrastructure.