ObamaCare. Then he walks out there a few hours later, standing by the famous Ohio clock, and says, cyber security, we should do it. It will take a lot longer to do than the time we have. If cloture is not invoked today, it is for reasons I have just enumerated but principally because of the Chamber of Commerce. They are opposed to the initial bill because it was mandatory that these companies do something to protect America from these attacks from bad people.

So Senators LIEBERMAN and COLLINS, the two managers of this bill from the Homeland Security Committee, said: OK. We don't think this is the right thing to do, but we will not make the provisions mandatory anymore. That is still not good enough for the Chamber of Commerce. A voluntary alternative is still something opposed by the Chamber of Commerce.

I have and numerous other people have come to the floor and talked about how important this bill is. The bill that is before this body now that we are going to vote cloture on would be a wonderful step forward. No, it doesn't do everything everyone wants, but it is a good bill. It is to protect our country. The leaders of the security of this Nation, including General Patraeus, General Dempsey, and the people working in NSA say this bill is more important than Iran, Afghanistan, Pakistan, and North Korea. But the Chamber of Commerce has now interjected themselves in the security of this Nation. They think they know more than Patraeus, Dempsey, and all the leaders of this country. They are telling the Republicans to vote against this, believing they will get something better later on. Maybe they will, but right now here is what we have. I think it sends a very bad message to the country that Republicans are not willing to support this legislation.

To show how serious the Republicans are to get this bill done, they filed an amendment on a right-to-work law and they filed an amendment on repealing Dodd-Frank. That is just some of the beginning volleys they shot over here. My friend, the Senior Senator from Arizona, steps in and says: We are working on a list.

So I am disappointed, perplexed, and somewhat confused about how the Republicans want to proceed. It is obvious—it is obvious—until they get a signoff from the chamber of commerce that nothing will happen on one of the most important security interests this country has faced in generations.

So I would suggest that the Republican leader, rather than trying to denigrate this legislation that has been done with the best interests of the country at heart—including one of his most valued Senators, Ms. COLLINS—do a conference call with the chamber of commerce. Have them come down here and tell them what they want, and maybe, with what the chamber of commerce wants, we can work something out, because they are ruling the place now as far as this legislation goes.

The chamber of commerce, I will repeat, for the first time that I am aware of in the history of this country, has now become the protector of our Nation's security interests. That says it all, Mr. President.

RESERVATION OF LEADER TIME

The ACTING PRESIDENT pro tempore. Under the previous order, the leadership time is reserved.

AFRICAN GROWTH AND OPPORTUNITY AMENDMENT ACT

The ACTING PRESIDENT pro tempore. Under the previous order, the Senate will proceed to the consideration of S. 3326, which the clerk will report.

The assistant legislative clerk read as follows:

A bill, (S. 3326), to amend the African Growth and Opportunity Act to extend the third-country fabric program and to add South Sudan to the list of countries eligible for designation under that Act, to make technical corrections to the Harmonized Tariff Schedule of the United States relating to the textile and apparel rules of origin for the Dominican Republic-Central America-United States Free Trade Agreement, to approve the renewal of import restrictions contained in the Burmese Freedom and Democracy Act of 2003, and for other purposes.

The ACTING PRESIDENT pro tempore. The Senator from Oklahoma.

Mr. COBURN. Mr. President, first of all, I wish to say I appreciate the leadership for working to ensure a vote on this package. This package was slowed down not because anybody is truly opposed to what we are trying to do, but the package was slowed down because of the way we are paying for it. We are going to see that coming over from the House as well. It is not a Republican or a Democratic problem; it is a problem of all of us because there is going to be an emergency farm bill, a disaster bill, coming over that is going to spend almost $400 million, and it is paid for over 5 years. That has to stop. It has to stop.

Right now, in this country, every man, woman, and child is on the hook for $53,000 of debt. So the typical American family is on the hook for 212,000 bucks right now because of what we have done. So my objection was not with the AGOA package, it is not with Myanmar, it is not with any of that. Those are great policy things. My objection is we are addicted to not fulfilling our responsibilities and delaying.

So this is a very simple, straightforward message and amendment that does two things: One, it recognizes the recommendation of the Obama administration in terms of duplication and the need for consolidation. That is how we are eventually going to get out of the hole. We have $130 trillion in unfunded liabilities, and we have $16 trillion in debt. It was a good recommendation. We totally ignored it. We have ignored it. Nothing has happened on what they have recommended. There have been no hearings on what the Obama administration recommended in terms of combining some of the departments at OMB.

So this is just a step toward trying to meet in the middle with what the Obama administration has recommended and us actually paying the $200 million in costs over 2 years, with $200 million worth of savings in 2 years.

The bill, as it presently stands, takes 10 years to pay for $200 million. We have a $3.7 trillion budget—or CR—and we can't find—it is less than one-hundredth of 1 percent, and we can't find it. So what this does is delay the cost—the payment—for this bill over a period of years, all the way out to 2023. No family who is broke gets to operate that way—and we are. Nobody who has maxed out their credit cards gets to do that, and we have maxed them out. So what we are saying is there is a ton of money that is available that we can use.

We have had three amendments on this floor that everybody who is going to be in opposition to this have voted for to eliminate duplication. The vast majority of my colleagues on the other side have voted for it, and the vast majority of my colleagues on my side have voted for it. So we are going to use that same skill where we know there is waste and we know there is inefficiency. We have tons of GAO reports, tons of IG, and tons of oversight of the Homeland Security Committee in the Senate that shows where the duplication is. All we are asking is, let's pay for it. Let's pay for it.

This place is so manipulated, I couldn't get a score until yesterday because somebody was telling them don't give him a score. Then when we changed the amendment, all of a sudden, because we want to know what the amendment says, CBO says: Well, wait a minute. That might not work. The fact is CBO didn't read our amendment right, and they know they didn't. So OMB was consulted. They said this amendment is implementable, and it fits with what the President was recommending in terms of consolidation of programs.

So what it says is let's make this a start today. Let's actually start paying for things in the years in which we are going to spend the money, and let's not kick the can down the road. Let's not charge it to our kids because the history is we take 10 years to pay for something, we come back next year and we will change it. We will change it. So what was paid for this year all of a sudden is not paid for anymore, and it is smoke and mirrors for the American people.

So this is very straightforward. It is a clean pay-for. It uses two mechanisms to get there which have been scored that will accomplish it.

I fully support the AGOA. I am sorry we got delayed. I am actually sorry it took—because there has already been

some damage done, than had we passed it when it came here. That was never my intent, but we can right that today. What I agreed to is if I lose the amendment, fine. But to not try to pay for things, to not create a discipline to get back where we should be—we are going to do this. We may not do this today, but I promise my colleagues the international financial community, in a very short period of time, is going to make us do this. So let's start doing it on our own under our own terms rather than what some foreign bondholder or the Chinese want to do.

The other objection that might be there is, well, if we do this, it will have to go back to the House. That is right. This passed on suspension. There was very little opposition to it. It will go back modified; they will pass it. I have talked to the Speaker. They haven't passed the other one first because they are waiting on us to act. We will hold ours at the desk because it has a revenue problem; they will modify theirs; they will do exactly what we did. I would just appreciate us standing up to the real problems in front of us.

It is a great goal to want to help these areas. It is a great goal to put the sanctions back on Myanmar so that they can be adjusted and used to create freedom. Those are great goals. But there is a greater goal because none of those things are going to matter if our financial system, our way of life, crashes around us because we are not responsible here.

I reserve the remainder of my time.

The ACTING PRESIDENT pro tempore. Does the Senator wish to call up his amendment?

Mr. COBURN. I do. I thank the Chair.

AMENDMENT NO. 2771

The ACTING PRESIDENT pro tempore. The clerk will report.

The assistant legislative clerk read as follows:

The Senator from Oklahoma [Mr. COBURN] proposes an amendment numbered 2771.

Mr. COBURN. I ask unanimous consent that the reading of the amendment be dispensed with.

The ACTING PRESIDENT pro tempore. Without objection, it is so ordered.

The amendment is as follows:

(Purpose: In the nature of a substitute)

Strike all after the enacting clause and insert the following:

SECTION 1. AMENDMENTS TO AFRICAN GROWTH AND OPPORTUNITY ACT.

(a) EXTENSION OF THIRD-COUNTRY FABRIC PROGRAM.—Section 112(c)(1) of the African Growth and Opportunity Act (19 U.S.C. 3721(c)(1)) is amended—

(1) in the paragraph heading, by striking ''2012'' and inserting ''2015'';

(2) in subparagraph (A), by striking ''2012'' and inserting ''2015''; and

(3) in subparagraph (B)(ii), by striking ''2012'' and inserting ''2015''.

(b) ADDITION OF SOUTH SUDAN.—Section 107 of that Act (19 U.S.C. 3706) is amended by inserting after ''Republic of South Africa (South Africa).'' the following:

''Republic of South Sudan (South Sudan).''.

(c) CONFORMING AMENDMENT.—Section 102(2) of that Act (19 U.S.C. 3701(2)) is amended by striking ''48''.

(d) EFFECTIVE DATE.—The amendments made by this section shall take effect on the date of the enactment of this Act.

SEC. 2. ELIMINATION OF UNNECESSARY DUPLICATION, REDUNDANCY, AND OVERLAP OF FEDERAL TRADE PROGRAMS.

Notwithstanding any other provision of law, the Director of the Office of Management and Budget shall coordinate with the heads of the relevant Federal agencies—

(1) to, not later than 60 days after the date of the enactment of this Act, eliminate, consolidate, or streamline Federal programs and Federal agencies with duplicative or overlapping missions relating to trade;

(2) to, not later than September 30, 2012, rescind the unobligated balances of all amounts made available for fiscal year 2012 for programs relating to trade for the Department of Commerce, the Small Business Administration, the Export-Import Bank of the United States, the Overseas Private Investment Corporation, and the Trade and Development Agency, with the amounts rescinded to be deposited in the general fund of the Treasury for purposes of deficit reduction;

(3) to reduce spending on programs described in paragraph (2) by not less than $192,000,000 in fiscal years 2012 and 2013 (including the amounts rescinded pursuant to paragraph (2)); and

(4) to report to Congress not later than 180 days after the date of the enactment of this Act with recommendations for any legislative changes required to further eliminate, consolidate, or streamline Federal programs and Federal agencies with duplicative or overlapping trade missions.

The ACTING PRESIDENT pro tempore. Who yields time?

The Senator from Delaware.

Mr. COONS. Mr. President, I rise today to speak both in favor of the passage of the bill, S. 3326, and to speak against the Coburn amendment.

I, first, wish to thank Leaders REID and MCCONNELL, as well as Senators BAUCUS and HATCH, for working together diligently to find a path forward for passing this bill. I wish to recognize Senator COBURN and Senator MENENDEZ for being willing to work with us to get to today.

I say with some regret that I stand to speak against the Coburn amendment because I respect and recognize Senator COBURN's determination to hold this body accountable and to find pathways forward to deal with our record deficit and debt. In that broader objective, I look forward to working with him on finding responsible pay-fors in future bills and in finding ways that we can steadily partner to reduce the deficit and to find and root out waste and abuse in Federal spending. But I have to say in this particular case, on this amendment, on this day, if we change the pay-for, we kill the bill.

We have heard clearly from the Republican chairman of the House Ways and Means Committee, Mr. CAMP, and from his ranking minority member, Congressman LEVIN, that they will not take up this bill if amended in this form, if broken and reassembled, or if sent over in any other way. The pressure of today and the pressure of the value, the importance of this bill is what I choose to speak to. I may at some point reserve time to speak to other issues embedded in the amendment, but I first wanted to speak to the underlying bill.

I am the chairman of the African Affairs Subcommittee of the Senate Foreign Relations Committee, and it is, in some ways, my special honor and challenge to help this body grasp why the African Growth and Opportunity Act is important for us to reauthorize today. Specifically what I am speaking to is the third-country fabric provision which expires in September. This Chamber is about to go out of session later today, and every day we delay in the reauthorization of this critical provision costs jobs, costs opportunity, and costs the future. Let me speak to that for a few minutes, if I might.

Creating American jobs and fueling our economic recovery is my top priority, and I know it is for many Members of this body. That is why I am here to talk about what we can do to strengthen our economic security. It may surprise my colleagues, but the truth is one of the best ways to look for that future opportunity is one that was considered among the least likely just a few years ago in Sub-Saharan Africa.

Access to emerging markets is critical to America's health and growth, and increased political stability and rising wages in an emerging middle class across Africa makes it the most promising continent for countries willing to invest in long-term partnerships with the United States. In AGOA—the African Growth and Opportunity Act—and its third-country fabric provision, the United States has seized this opportunity to pursue broad and mutually beneficial economic relationships that give American consumers and businesses economic security by allowing eligible countries to export apparel from Africa that is more affordable to the American consumer and, in so doing, create jobs in Africa that otherwise would be elsewhere in the world.

This key provision, as I have said, expires in September. Our delay in moving forward with reauthorization that has earned strong bipartisan support is already disrupting production for American apparel companies along with the supply chain on which their customers depend. In my view, we cannot wait to take action. America can't afford to turn its back on African markets, and Congress can't afford to turn its back on extending this provision.

Every 3 years since 2000, Congress has unanimously passed the reauthorization of this provision without controversy, and it is, in my view, time to do so again.

I respect Senator COBURN's concern that we must change business as usual in this Chamber, but the timing of this amendment and the timing of this concern is, to me, not wise.

Today Secretary Clinton is in the middle of a continent-wide tour of African countries. She is engaging with

countries for strong emerging middle classes, and that offers us great opportunity: future economic partnership and very real political partnerships. From Ghana to Ethiopia to Tanzania to a half dozen other countries, some of the fastest growing economies in the world are in Sub-Saharan Africa. The seven countries that are the fastest growing economies in Sub-Saharan Africa are home to 350 million potential consumers of our products. In my view, that is why I am urging my colleagues to vote against the Coburn amendment and to allow us to pass this critically important bill today. Failing to do so, in my view, is bad for Africa and for America.

Reauthorizing this provision supports the poorest African workers, the vast majority of them women. Senator ISAKSON, who is my capable and talented ranking minority member on the African Affairs Subcommittee, joined with Congressman SMITH and Congresswoman BASS, who are our counterparts in the House, in hosting a meeting 3 months and 6 months ago with roughly 35 Ambassadors from all over the continent who pleaded with us to reauthorize this critical provision.

The economic benefits of a strong middle class in Africa are obvious—a pool of new consumers hungry for American products; potential partners for us. And countries with flourishing middle classes are more likely to have strong democratic institutions, good governance, and low corruption. They are more likely to be stable and bulwarks against instability in Africa, a region that I think is vital to our future.

In short, then, reauthorizing this provision and continuing our strong bipartisan support of tradition for AGOA is where the United States can continue to differentiate itself from competitors such as China, which recently surpassed the United States as Africa's No. 1 trading partner. The United States has exports to Sub-Saharan Africa that exceeded $21 billion last year, growing at a pace that exceeds our exports to the rest of the world.

Africans want to partner with us. They want to work with us, and they seek opportunity. This sort of bipartisanship that in the past has allowed this AGOA third country fabric provision to be reauthorized without controversy is one that I think we should embrace again today. So let's end the delays and reauthorize this provision.

Mr. President, I yield 3 minutes of my time, if I might, to the Senator from Georgia, who would like to speak to the issue of the value of the African Growth and Opportunity Act.

Mr. ISAKSON. Mr. President, may I inquire of the Chair how much of the proponents' time would that 3 minutes leave?

The ACTING PRESIDENT pro tempore. Five minutes.

Mr. ISAKSON. Thank you, Mr. President.

The ACTING PRESIDENT pro tempore. The Senator from Georgia is recognized.

Mr. ISAKSON. Mr. President, I rise for just a moment to do two things. First of all, I spent 33 years selling houses. I have dealt with honest brokers, and I have dealt with brokers who were hard to deal with and whom I would never categorize as honest. Senator COBURN from Oklahoma is the most honest broker I have ever dealt with in politics or in selling houses. I wish to acknowledge for just a second exactly what he said about the process, his support for the AGOA provisions but his concern about the pay-for, but the fact that he never tried to scuttle this piece of legislation, he only tried to get his day in court. I respect that, and I want him to know that. If we all acted a little bit more like that, we would have a lot more debate on the floor and a lot fewer problems in terms of running our country.

As far as AGOA, I want to say this. As the chairman and ranking member, as Senator COONS and I are, of the African Affairs Subcommittee, we travel to that continent quite a bit. One of my trips was to the Sudan, to Darfur, and to the South Sudan, when the comprehensive peace agreement was being negotiated. As this body knows, the South Sudan had their revolution peacefully. South Sudan became the newest country on the face of this Earth, and South Sudan will become, if AGOA passes today, one of the parties to this agreement, which is critical to the developing economy of the South Sudan as an independent nation. Further, the other nations that are included are nations that depend on this legislation to raise a middle class in Africa that will become the customers of the United States of America and our businesses.

I say often in my speeches about Africa that if it is true that Europe was the continent of the 20th century in the first 50 years and if it is true that Asia was the most important continent in the last 50 years of the 20th century, Africa is the continent of the 21st century. This is an agreement that is important to our relationship with Africa, it is important to our economy, it is important to American textiles, and it is important to jobs in Africa.

I commend Senator COONS for his hard work, and I intend to support the AGOA bill and ask all of my fellow colleagues to do the same.

I yield back.

The ACTING PRESIDENT pro tempore. The Senator from Oklahoma is recognized.

Mr. COBURN. Mr. President, it is intriguing to me. We heard the Senator from Delaware absolutely assure us that if we defy this, the House is not going to do the right thing. My conversation with Chairman CAMP was different from that. I do not know what the timing was between our conversations. But it is never the right time in Washington to fix our problems.

We do a lot of great things. You want to talk about job creation? Job creation has decreased by 1 million jobs a year in this country simply because we continue to add to our debt. And this bill adds to our debt. It is not paid for. It has another trick in there that actually charges more in corporate taxes just to get around pay-go.

So the point is—and I will not have any more to say on this bill so we can go on and get to the other—the point is, if we stood and did the right thing and led this country by actually paying for something at the time, the House would change it—just for the very reasons the Senator from Delaware said. It is important. If we had a strong vote that said: Yes, it is important, but, by dingy, we are not going to keep doing the same thing that has been bankrupting this country—but now we use an excuse to say: Well, here is our reason why we cannot do what is right.

America should spit us out of their mouth. We never find the right time to actually have the fiscal discipline that will solve our county's problems and create a viable future for our children, let alone African children.

So that is a real choice today. I do not expect to win this because this place is not going to change until the people who are here decide that the future of our country is more important than anything else and we start acting like it. And we can do good things internationally, but we can do them the right way that will not put our children at risk. Our debt level is such that our GDP is decreased by 1 percent right now—it is proven—just because of the amount of debt we have.

So we are going to pass a bill with great intentions, with which I agree. It will have a great result; I agree with that. We can do both. We can actually do better. But it is because there is not the spine in the Senate to stand up and make the hard choice. This country is full of people outside of Washington who are used to making hard choices, and they are doing it in this tough economic time all the time. They are making hard choices. We lack the intestinal fortitude to do that. We should have them here and us home because they know how to get it done.

So what we are going to do is we are going to do the same thing we have always done. We are not going to make the hard choice. We are not going to do the best we can do. We are going to settle for second best because we have an excuse not to make the hard choice. The excuse right now is that the House will not move. Well, I will guarantee you, if it as important as Senator COONS and Senator ISAKSON say it is, and Representative SMITH, and we sit here and say our position is that it is paid for within 2 years, I will bet you by tomorrow it will be paid for within 2 years. But we will not ever do that because we lack the courage to do the hard thing, the right thing. What has that gotten us? It has gotten us deeper in debt, a depressed economy, an anxious American citizenry that has no

confidence about the future, which is so self-fulfilling in terms of driving the economy down even further.

It is time for us to lead. This is a small issue, but if we cannot even pay for $200 million over 2 years, we do not deserve to be here, we do not deserve it, because what we are really doing—we are helping people in Africa, we are helping the freedom in Burma, but what we are really doing is taking just a little bit of freedom away from our kids. That is the real vote here. It is really not about money; it is about destroying the future prospects of this country because we refuse to make a hard choice.

There can be a lot of flowery speeches about it. We can say we are going to do something good. I will tell you that well-intentioned desires by the Members of this body are what has us $16 trillion in debt.

I will not spend any more time. I have the greatest respect for the Senator from Delaware. I know he believes in this cause. He is bigger than this. He can make this tough vote. He knows how big the problems are. If we are not going to do it now, when are we going to do it? If we are not going to do it on something small, when are we going to do it?

We are not going to do it, and that is what the American people get. That is why there is an uprising in this country to get back to the basics of the Constitution. That is why there are people who are interested—because we have mismanaged it because we will not do the hard part.

Mr. President, I yield back my time.

I will ask for the yeas and nays at the appropriate time.

The ACTING PRESIDENT pro tempore. The Senator from Delaware is recognized.

Mr. COONS. Mr. President, I wish to thank my colleague from Oklahoma for his remarks.

If I might just conclude my comments on this amendment by speaking in a little detail on the amendment and its substance.

The Senator from Oklahoma essentially directs the administration to find $192 million in reductions in spending in the following agencies: the Department of Commerce, the Small Business Administration, the Export-Import Bank, the Overseas Private Investment Corporation, and the Trade and Development Agency.

In my role as the chair of the African Affairs Subcommittee, we recently held a hearing on expanding U.S. trade opportunities in Africa for exactly the reasons I elucidated previously: that there is enormous growth, there are great opportunities across the continent. Our competitors from all over the world—not just China but Brazil, Russia, and other European countries—are expanding their investment and their seizure of these opportunities in a way that we are not.

The structure of this amendment would simply declare that there is $200 million of waste and duplication at several important trade agencies and direct the administration to slash their budgets for that amount and then hope for the best.

That is what Senator COBURN's proposed offset would do. These are agencies that promote and finance U.S. exports and help small and large U.S. businesses export and compete in a global market. In my view, exports, particularly to this market, mean jobs. So I am not convinced that now is the time to blindly slash our ability to export. I think we should instead be encouraging exports.

In the context of the Federal budget, $192 million is a very, very small amount of money. I look forward to working with Senator COBURN to find other places where we can find reductions of this size. But this amendment, at this time, on this day, would kill the broader and more important objective of reauthorizing the African Growth and Opportunity Act third-party fabric provision, of moving forward with relevant Burma sanctions, and of moving forward with an important technical fix to CAFTA.

This is a carefully crafted compromise bill that the House will pass once we pass it. I urge my colleagues to vote against the Coburn amendment and to move forward with passage of this vital bill.

Mr. President, I yield back the remainder of my time and yield the floor.

CYBERSECURITY ACT OF 2012

The ACTING PRESIDENT pro tempore. Under the previous order, the time until 11 a.m. will be equally divided and controlled between the two leaders or their designees.

The Senator from Maine is recognized.

Ms. COLLINS. Mr. President, later this morning we will vote on whether to invoke cloture on a major cyber security bill. In the past 3 days we have received letters from GEN Keith Alexander, who is the head of Cyber Command as well as the chief of the National Security Agency, from the Secretary of Homeland Security, and from the Chairman of the Joint Chiefs of Staff, urging us to act immediately on this important legislation. Let me read briefly from all three of these letters.

General Alexander said the following:

I am writing to express my strong support for passage of a comprehensive bipartisan cyber security bill by the Senate this week. The cyber threat facing the Nation is real and demands immediate action. The time to act is now; we simply cannot afford further delay.

That is what General Alexander has told us.

Secretary Napolitano wrote to us:

I am writing to express my strong support for S. 3414, the Cybersecurity Act of 2012. I can think of no more pressing legislative need in our current threat environment.

The Chairman of the Joint Chiefs of Staff, General Dempsey, wrote the following:

I am writing to add my voice to General Alexander's and urge immediate passage of comprehensive cyber security legislation. We must act now.

How many more implorings do we need from our Nation's top homeland and military officials to act on what many believe to be the greatest threat that is facing our Nation? A cyber attack with catastrophic consequences is a threat to our national security, our economic prosperity and, indeed, to our very way of life. Our adversaries have the means to launch a cyber attack that would be devastating to our country. All the experts tell us, it is not a matter of if a cyber attack is going to be launched, it is when it is going to occur.

So I find it incredible and indeed irresponsible that this body is unable to reach an agreement to allow us to move forward on this important legislation. It is astonishing to me that irrelevant, nongermane amendments have been filed to this important bill on both sides of the aisle. It is unacceptable that we have worked hard and have come up with a list of relevant and germane amendments, and yet we cannot seem to reach an agreement to proceed.

American officials—our government officials—have already documented that our businesses are losing billions of dollars annually and millions of jobs due to cyber attacks, attacks that are happening on our government and business computers and individual computers each and every day.

Yet our defenses are not there. General Alexander, who knows more about the cyber threat than any individual in this country, was asked to rank our preparedness for a large-scale cyber attack on a scale of 1 to 10. Do you know what he said? He deemed us to be at a 3. Is a 3 adequate to protect this country from what we know is coming, that is only a matter of time?

There have been all sorts of suggestions for improving this bill. We have adopted many of those suggestions. Indeed, we have made major changes to make this bill more acceptable to those on my side of the aisle. And what has been our reward? To be criticized for making changes in the bill, for having Members on our side of the aisle, my side of the aisle, say, well, now it is a different bill.

Well, it is a different bill because we took their suggestions, and we took the suggestions of a bipartisan group acting in good faith headed by Senator KYL and Senator WHITEHOUSE. There is much more I want to say on this issue. I see the chairman has arrived on the floor. I know opponents to the bill such as Senator HUTCHISON wish to speak and should certainly be given the right to do so. But let me say that rarely have I been so disappointed in the Senate's failure to come to grips with a threat to our country that all of these officials have warned us over and over again is urgent and must be addressed now. Not maybe in September; not probably by the end of the year; not in the next Congress, but now.

The ACTING PRESIDENT pro tempore. The Senator from Texas is recognized.

Mrs. HUTCHISON. Mr. President, I wanted to get the time for our side and the time for the bill sponsor's side and clarify that the people on our side would have 15 minutes. Is that correct?

The ACTING PRESIDENT pro tempore. The time is divided between the two leaders or their designees. The Republican side has approximately 9 minutes, and the majority side has 16 minutes.

Mrs. HUTCHISON. I wanted to clarify that there would be time for the opposition side. I did not know if Senator COLLINS is speaking for the majority side then or the minority side. I am trying to clarify to assure that the opposition is getting some equal amount of time or close to equal.

Mr. LIEBERMAN. Mr. President, I understand the time is divided between the two leaders. But I think there is 15 minutes for the proponents and for those opposed. I would ask unanimous consent that that be the case.

The ACTING PRESIDENT pro tempore. Is there objection?

Ms. COLLINS. Reserving the right to object, it is my understanding that I am managing the time on the Republican side. I, of course, want to make sure that the Senator from Texas is treated fairly and is given an opportunity to present her views. But it was my understanding that the 15 minutes is allocated to me to dole out or to allocate on our side.

Mrs. HUTCHISON. Then how much time would the proponents have with Senator COLLINS and Senator LIEBERMAN on the proponents' side?

The ACTING PRESIDENT pro tempore. The time is divided between the two sides, not between the proponents and opponents.

Mrs. HUTCHISON. How much, then, would be left on the Republican side?

The ACTING PRESIDENT pro tempore. There is 7 minutes left on the Republican side. The majority side has 15.

Mrs. HUTCHISON. Mr. President, I would ask unanimous consent that the opponents have at least 10 minutes.

Ms. COLLINS. I have no objection.

Mr. LIEBERMAN. Nor do I.

The ACTING PRESIDENT pro tempore. Without objection, it is so ordered.

The Senator from Texas.

Mrs. HUTCHISON. Mr. President, I wish to be notified when I have 5 minutes left, because Senator MCCAIN is expected on the floor, and if Senator CHAMBLISS or others come, I would like to have the time.

The PRESIDING OFFICER. The Chair will do so.

Mrs. HUTCHISON. Mr. President, I rise to express my disappointment that we are taking a vote that is very premature. Not that we have not been discussing this bill for over a year. I have certainly been one of the first to say that we should vote on a cyber security bill. This is a complicated bill. It is a bill that did not get marked up in committee.

In our discussions, we are talking about amendments. I want to say that the proponents of the bill before us have certainly been willing to talk and adjust and try to make changes in the bill. It is not there yet even though we have been meeting pretty much constantly. There are three different groups that have a very strong interest. All of us are interested in getting a cyber security bill, but none of us likes what is before us—well, obviously the proponents of the bill like what is before us.

But two other groups are very concerned about further needs in the bill. Let me say that we have an alternative called SECURE IT. It is cosponsored by eight of the ranking members of committees and subcommittees that have jurisdiction over cyber security. Senators MCCAIN, myself, CHAMBLISS, GRASSLEY, MURKOWSKI, COATS, BURR, and JOHNSON are cosponsoring a bill that could pass the House and go to the President.

My concern with S. 3414, on which we are voting on cloture, is on the process, because we have not had a chance to amend this bill. The majority leader is attempting to invoke cloture and fill the tree so that we are not able to put any amendments on this bill at all. It is a bill that will not get 41 votes for sure. And there are many others who are very concerned about the substance of the bill.

You cannot have a bill with no amendments that is this important and this technical. Let me state some of my concerns on the bill before us. First, it will actually undermine the current information sharing between the government and the private sector. The biggest priority we have is to get the private sector to the table and to make sure they have the ability to not only give information to the government but get information from the government. Furthermore, they must be able to share among the other industries, if they see a cyber threat, on an expedited basis.

No. 2, the Department of Homeland Security would be granted authority over standard setting for private sector systems. That is unacceptable in the private sector and most certainly is not going to produce what is a consensus for getting the information we need. It assumes that government must take the adversarial role against private network owners in order to get cooperation when, in fact, both the government and the private sector share the same goals of increased cyber security.

Let me read from a couple of letters we have received with concerns about this bill. The American Bankers Association, the Financial Services Roundtable, the Consumer Bankers Association, and 6 other organizations say: This legislation threatens to undermine important cyber security protections already in place for our customers and institutions. It misses an opportunity to substantially improve cyber threat information sharing between the Federal Government and the private sector.

The National Association of Manufacturers says: The creation of a new government-administered program in an agency yet to be named forces unnecessary regulatory uncertainty on the private sector.

The defense industry groups are very concerned about not having direct access to the National Security Agency with whom they deal now, and this bill would take that away from their capabilities.

The ACTING PRESIDENT pro tempore. The Senator has 5 minutes remaining.

Mrs. HUTCHISON. Let me ask my colleagues, I have reserved the 5 minutes that I have for opponents. Is that going to change, Senator LIEBERMAN? If not, I will give 2½ minutes each to Senator MCCAIN and Senator CHAMBLISS of my 5 minutes.

Mr. LIEBERMAN. Mr. President, I think that is the situation we are in, because the vote is set to go off in a little more than 15 minutes. I have not spoken yet.

Mrs. HUTCHISON. I will ask my colleagues, Senator MCCAIN—I can give you 2½ minutes to you and Senator CHAMBLISS. While they are going to their microphones, I want to say that they have been instrumental in trying to get a consensus bill. And they, like myself, are very disappointed that we are prematurely voting on a cloture motion when we have had no ability to amend the bill.

I yield 2½ minutes to Senator MCCAIN.

The ACTING PRESIDENT pro tempore. The Senator from Arizona is recognized.

Mr. MCCAIN. Well, Mr. President, I want to again thank Senator LIEBERMAN and Senator COLLINS for their willingness to negotiate seriously. I want to thank also Senator CHAMBLISS as well as Senator HUTCHISON and many others, Senator KYL and others.

We have had large meetings, small meetings, medium-sized meetings. We have had discussions among various groups. I believe we sort of had the outlines of a framework that we could have had a certain number of amendments that we all agreed to that would be voted on. At the same time, we could prevail upon some of our colleagues not to have nongermane amendments.

Unfortunately, the first amendment proposed by the majority leader has to do with tax cuts. Look, I say to my colleagues that I think we have developed a framework where we can move forward with a certain number of germane amendments. All of us appreciate how important this issue is.

I don't see the need for this vote. Cloture will not be invoked. All it will do is embed people in their previously held positions. What we should be

doing is continuing productive negotiations and discussions that we had all during yesterday, put off this cloture vote, and try to come to some agreement in recognition that cyber security is a vital national security issue. We all recognize that. We started out very much poles apart. I think there have been some agreements made which I view as significant progress.

I regret, I say to Senator LIEBERMAN, Senator COLLINS, and all my colleagues, that we are taking this vote when we should be spending our time—at least the rest of the day—setting up a framework that we can address cyber security during the first week we are back in September. But it is what it is.

I thank Senators LIEBERMAN and COLLINS for their willingness to sit down and negotiate. We still have significant differences, but I think those could have been resolved. I hope this vote doesn't have a chilling effect on what I think was progress that was being made.

The ACTING PRESIDENT pro tempore. The Senator's time has expired.

Mr. MCCAIN. On issues of transparency and information sharing and others, there are still differences, but they have been narrowed. Again, I thank my colleagues for their hard work.

The ACTING PRESIDENT pro tempore. The Senator from Georgia.

Mr. CHAMBLISS. Mr. President, let me add to what Senator MCCAIN has said. We have been working very hard with the sponsors of the bill, Senators LIEBERMAN and COLLINS, who have been receptive and open to our dialog over the last several days and weeks. It is an indication, No. 1, that everybody in this body recognizes the seriousness of this issue, but it is also a recognition of the complexity of this issue. There are about four or five committees of jurisdiction that have a piece of the issue of cyber security and, unfortunately, we didn't go through the regular order of giving all those committees the opportunity to go through the regular markup process. That may or may not have solved some of the issues we are now dealing with. But we are down to the final minutes before a cloture vote.

Unfortunately, I will vote against cloture and I recommend that my colleagues do likewise and that we continue over this break to negotiate on the remaining issues we have. They have been narrowed in number and scope. Both sides are negotiating in good faith because we all understand this is an issue of such critical importance.

The basic philosophical difference we have is that we all seek to protect the private sector from cyber attacks that may have a huge impact on life or on our economy. The issue is, primarily, does the government know better how to do that or does the private sector know better how to protect itself, as we think it does. While we understand the government has a role to play, we have capabilities and capacities within the Federal Government that the private sector doesn't have, and we recognize that. That is why we have been negotiating in good faith to try to find that common ground between the government and the private sector to ensure the protection of the basic critical infrastructure in this country.

I thank the Chair and yield the floor.

Mrs. HUTCHISON. Mr. President, I ask unanimous consent to have printed in the RECORD the two letters from which I read in my statement and an article from the Wall Street Journal this morning on this issue.

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

AUGUST 1, 2012.

Hon. HARRY REID,
Majority Leader, U.S. Senate,
U.S. Capitol, Washington, DC.
Hon. MITCH MCCONNELL,
Republican Leader, U.S. Senate,
U.S. Capitol, Washington, DC.

DEAR MAJORITY LEADER REID AND REPUBLICAN LEADER MCCONNELL: The financial services industry, represented by the undersigned organizations, opposes the Cybersecurity Act of 2012 (S. 3414) in its current form. While we strongly support efforts to protect the nation's critical infrastructure from cyber-attacks, this legislation threatens to undermine important cybersecurity protections already in place for our customers and institutions, and misses an opportunity to substantially improve cyber threat information-sharing between the federal government and the private sector.

Our sector recognizes the very real and ongoing threat of cyber-attacks and works very hard to prevent those attacks by constantly updating, and investing heavily in our security systems. We work tirelessly, day and night, to block cyber-attacks, including working with the federal government and other private sectors to share information and design effective ways to mitigate cyber threats. Given this, we believe any legislation passed by the Senate, and eventually enacted into law, must take a balanced approach that builds upon, but does not duplicate or undermine what is already in place and working well in the financial sector. At the same time, it should enhance Cybersecurity protections in areas where they are most needed.

There are several issues and questions raised by the technical language included in the revised bill. For instance, while the sponsors of the legislation have attempted to design a voluntary framework for the designation of ''critical infrastructure,'' the text of the bill would likely create a mandatory regulatory regime that could displace robust efforts already being made in the financial sector to combat the risk of cyber-attacks. Additionally, the government agency ''Council'' created in Title I of the bill to conduct risk assessments, and set best practices for protecting critical infrastructure does not provide a meaningful role for sector-specific agencies that oversee financial institutions. The bill does not recognize the existing security standards and regulations to which financial institutions are subject, including the Gramm-Leach-Bliley Act, nor the regular oversight and examinations conducted by financial regulatory agencies. This opens the door for inconsistent and potentially duplicative regulations that are more than likely to become mandatory for our industry.

Further, the process for designating financial systems as covered critical infrastructure does not provide for meaningful input of financial agencies or the private sector, and this is crucially important for determining what is, in fact, critical and what is not. Finally, we are concerned that the changes made to the Title VII information sharing provisions could actually restrict some forms of important information sharing between the government and private sectors, as well as decrease the current level of information sharing between private entities.

As the Senate considers S. 3414, a legislative proposal we support could be considered as an amendment on the Senate floor; specifically, Amendment #2581 offered by Senators Hutchison and McCain, which encompasses the SECURE IT Act of 2012 (S. 3342). This amendment would provide necessary updates and clarifications to current law that will facilitate and increase cyber intelligence information sharing within the private and public sectors, as well as update the federal information security policy, encourage research and development, and increase criminal penalties. We encourage you to support this amendment, which builds upon our existing regulatory structure, better protecting financial institutions and our customers.

We recognize that more needs to be done to encourage high levels of cybersecurity protection across all sectors deemed critical infrastructure. We would like to continue to work with you and your colleagues in the Senate to pass legislation that accomplishes this goal, while utilizing existing regulatory requirements and ensuring a central role for sector-specific agencies; this would bolster the ongoing efforts of the financial services industry as we continue to improve the effectiveness of our cybersecurity.

We look forward to working with you and your colleagues on this important issue.

American Bankers Association, American Council of Life Insurers, The Clearing House Association, Consumer Bankers Association, Electronic Funds Transfer Association.

Financial Services Information Sharing and Analysis Center (FS-ISAC), The Financial Services Roundtable, NACHA-The Electronic Payments Association, Securities Industry and Financial Markets Association (SIFMA).

NATIONAL ASSOCIATION
OF MANUFACTURERS,
July 25, 2012.

Hon. HARRY REID,
U.S. Senate, Hart Senate Office Building,
Washington, DC.
Hon. MITCH MCCONNELL,
U.S. Senate, Russell Senate Office Building,
Washington, DC.

DEAR MAJORITY LEADER REID AND MINORITY LEADER MCCONNELL: On behalf of the 12,000 members of the National Association of Manufacturers (NAM), the largest manufacturing association in the United States representing manufacturers in every industrial sector and in all 50 states, I am writing to express the NAM's concern with S. 3414, the Cybersecurity Act of 2012 scheduled to be considered by the Senate this week and reiterate our support for S. 3342, the SECURE IT Act, cybersecurity legislation that includes consensus-based provisions supported by manufacturers.

As currently written, S. 3414 raises significant concerns for our members. While we support increasing information sharing and reducing companies' liability, the legislation unfortunately does not allow manufacturers to share information among themselves and also receive liability protection. It requires companies to share that same information jointly with a new government entity created in the legislation to receive the benefit of liability protection. The creation of a new government-administered program in an agency yet-to-be-named forces unnecessary regulatory uncertainty on the private sector, creates a system that allows for new, overly prescriptive regulations, and is a disincentive to share information.

NAM members are also concerned that owners and operators of critical infrastructure would be subject to cybersecurity assessments by third-party auditors who are granted unfettered access to company information. This provision creates economic uncertainty as manufacturers are concerned that the release of proprietary information

to third parties could actually create new security risks. Manufacturers are already subject to agency and sector-specific regulations and requirements. They have well-developed compliance processes to improve their systems. More government mandates are unnecessary and would quickly become obsolete.

Manufacturers through their comprehensive and connected relationships with customers, vendors, suppliers, and governments are entrusted with vast amounts of data. They hold the responsibility of securing this data, the networks on which it runs, and the facilities and machinery they control at the highest priority level. Manufacturers know the economic security of the United States is directly related to our cybersecurity. The NAM and all manufacturers remain intensely committed to securing our nation's cyberinfrastructure and we look forward to working with you toward this goal.

Sincerely,

DOROTHY COLEMAN,
Vice President,
Tax and Domestic Economic Policy.

[From the Wall Street Journal, Aug. 1, 2012]

CYBER HILL BATTLE

SEARCHING FOR A COMMON SENSE DEFENSE AGAINST A ''DIGITAL PEARL HARBOR''

Every Washington politician and his favorite lobbyist claim to want to shore up America's cyber-defenses. So naturally Congress is mucking up efforts to protect financial systems and power grids from hackers, terrorists or rogue states.

The Senate is due to take up cyber-security legislation this week before its summer recess. The goal ought to be to find common ground with a modest, bipartisan bill passed by the House of Representatives in May. In this instance a delay to work out a compromise in the autumn is preferable to a hasty vote.

The Senate debate so far hasn't been encouraging. The White House supports legislation from Joe Lieberman, the Connecticut Independent, and Maine Republican Susan Collins. Their Cybersecurity Act of 2012 expands government oversight of private networks. Without further substantial changes, the bill has little shot of getting through a House-Senate conference.

John McCain, the Arizona Republican, has offered better alternatives. He wants to give companies a legal avenue to draw on the government's cyber expertise or share information about cyber threats with the FBI or National Security Agency. As in the House's Cyber Intelligence Sharing and Protection Act, this cooperation would be voluntary.

The Lieberman bill brings government compulsion. The Department of Homeland Security—that nimble bureaucracy—would draw up and enforce new ''minimum'' cybersecurity standards for private business. This mandate adds costs for government and the private economy. The same folks who give you invasive airport screening will now poke around IT departments. No wonder the Chamber of Commerce wants Homeland Security to keep its hands off ''our junk,'' so to speak.

Mr. Lieberman has softened some provisions. He dropped a mandate for private facilities to upgrade their cyber-security as prescribed by government. He took out a ''kill switch'' that lets the President shut down the Internet in an emergency. Yet he isn't going to win bipartisan support in both houses as long as any new standards for privately owned technology aren't voluntary.

Heeding the ACLU, the White House and Mr. Lieberman want strict limits on how government agencies can use intelligence garnered through the information-sharing program. Such artificial walls were in place before 9/11, which was why the CIA couldn't tell the FBI about suspected terrorists enrolled in American flight-training schools. The House and McCain versions allow the feds to act on information about, say, Iran's cyber-terror plans.

The White House cited privacy grounds in threatening to veto the House bill. Call us naïve, but we don't see how the voluntary sharing of selective data related to legally defined cyber threats constitutes an Orwellian surveillance program.

The House and McCain cyber-security proposals offer limited solutions to guard against a ''digital Pearl Harbor.'' In a world of fast-changing technology, less is better policy, and in this case it stands a far better chance of becoming the law of the land.

Mr. KYL. Mr. President, all of us recognize the need to strengthen our cyber security defense to protect our defense industrial base, financial sector, and government networks from nation states and independent hackers. GEN Keith Alexander, commander of the U.S. Cyber Command, said that he rates U.S. preparedness at 3 on a scale of 1 to 10. So it is important that Congress act responsibly to get this right.

I voted against invoking cloture on the cyber security bill because I believe cloture was filed too early. This is vast, far-reaching legislation that requires ample consideration time. Two days isn't enough. Moreover, Senators weren't even given a chance to offer amendments to improve the legislation, and the legislation wasn't marked up by a relevant committee.

I believe we can ultimately come together to find enough common ground so that we can pass a bill that can get through a House-Senate conference committee.

We have come a long way since talks began, and the negotiators have spent an enormous amount of time working on two key issues: critical infrastructure and information sharing between the government and the private sector. I am confident the good will exists to work out these differences.

To that end, it is my hope that we who are involved in the bipartisan negotiations can use the month of August to continue. Cyber security isn't a Republican or a Democratic issue. Let's work together to pass a bipartisan bill that the President can sign into law.

Ms. SNOWE. Mr. President, I rise today to express my strong support for finding a path to legislation that will at long last confront our Nation's 21st-century vulnerability to cyber crime, global cyber espionage, and cyber attacks. This legislation has been a long time in the making, and over the last several years I have been privileged to work with colleagues on the Senate Intelligence and Commerce Committees to address some of these consequential matters, including Senator ROCKEFELLER, whom I collaborated with closely on cyber security legislation that passed the Commerce Committee unanimously in 2010; Senator HUTCHISON, who has worked tirelessly with us on these issues as ranking member on the Commerce Committee; Senators MIKULSKI and WHITEHOUSE, with whom I served on the Intelligence Committee's Cyber Security Task Force; Senator WARNER, who has joined me in underscoring the urgency of considering cyber security legislation in a transparent and nonpartisan manner; and Senators LIEBERMAN and COLLINS, who have led the effort to craft this revised cyber security bill.

Nothing less than the very foundation of our national and economic security is at risk, and it is essential that we be prepared to defend against cyber activity that could cause catastrophic damage and loss of life in this country.

Still, some of my colleagues will undoubtedly make poignant and convincing arguments for why this Chamber should delay consideration of a comprehensive cyber security bill—stressing the complexity of the questions involved, the competing jurisdictions, and the many unknowns associated with a medium where innovation in functionality will continue to outpace innovation in security.

However, last fall the National Counterintelligence Executive warned that the rapidly accelerating rate of change in information technology and communications is likely to ''disrupt security procedures and provide new openings for collection of sensitive U.S. economic and technology information.'' In fact, the counterintelligence report cited Cisco Systems studies predicting that the number of devices such as smartphones and laptops in operation worldwide will increase from about 12.5 billion in 2010 to 25 billion in 2015.

Thus, as a result of this proliferation in the number of operating systems connected to the Internet, the Counterintelligence Executive has assessed that ''the growing complexity and density of cyber space will provide more cover for remote cyber intruders and make it even harder than today to establish attribution for these incidents.''

So as I said during the Senate Commerce Committee's bipartisan, unanimous markup of the Rockefeller-Snowe cyber security legislation over 2 years ago in early 2010, when it comes to the threat we face in cyber space, time is not on our side, and this is further evidence of that irrefutable fact.

This Congress could spend another 2 years debating the merits of various approaches and continuing to operate based on a reactive hodgepodge of government directives and bureaucratic confusion. But at the end of the day, the only way to begin preparing our Nation to defend against this emerging threat is to allow the Senate to work its will in a full and unrestrained debate.

In June, Senator WARNER and I urged the Senate's leadership to reach an agreement ensuring cyber security legislation receives an open debate on the Senate floor during the July work period. In calling for a fair amendment process, we in fact were simply repeating the cyber security debate commitment made by the majority leader at

the start of the year when he said that ''it is essential that we have a thorough and open debate on the Senate floor, including consideration of amendments to perfect the legislation, insert additional provisions where the majority of the Senate supports them, and remove provisions if such support does not exist.''

So I welcomed the majority leader's commitment to allow an open amendment process, and I joined my colleagues in voting to invoke cloture on the motion to proceed to the bill. As I have said repeatedly, only a bipartisan agreement will achieve our shared goal of passing cyber security legislation to prevent a devastating cyber attack.

That process must begin now, and as one who has served on the Select Committee on Intelligence for the last decade, I believe it is essential to begin by elucidating the nature of the indisputable threat we now face.

In June 2010, the Intelligence Committee's Cyber Security Task Force, on which I served along with Senators WHITEHOUSE and MIKULSKI, delivered its classified final report illustrating the myriad of challenges to the security of our physical, economic, and social systems in cyber space. I urge my colleagues to review this classified report.

As for some examples we can discuss in an open forum such as this, I encourage my colleagues to read the National Counterintelligence Executive's unclassified report to Congress entitled ''Foreign Spies Stealing U.S. Economic Secrets in Cyberspace.'' The Counterintelligence Executive's report, which was released last fall, is truly the authoritative document when it comes to portraying in detail the nature of the threat and its ramifications on our lives and—increasingly—our livelihoods. s

The report is incredibly eye-opening and represents the first time in which our government has explicitly named China and Russia as the primary points of origin for much of the malicious cyber activity targeting U.S. interests. In fact, the report states that the Governments of China and Russia ''remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace'' and it links much of the recent onslaught of computer network intrusions as originating from Internet Protocol addresses in these two countries.

For example, the Counterintelligence Executive's report cites a February 2011 study attributing an intrusion set called ''Night Dragon'' to an IP address located in China. According to the report, these cyber intruders were able to exfiltrate data from computer systems of global oil, energy, and petrochemical companies with the goal of obtaining information on ''sensitive competitive proprietary operations and on financing of oil and gas field bids.'' As the report notes, such activity on behalf of our economic rivals undermines the U.S. economy's ability to ''create jobs, generate revenues, foster innovation, and lay the economic foundation for prosperity and national security.'' And the report estimates that our losses from economic espionage range from ''$2 billion to $400 billion or more a year,'' reflecting the scarcity of data and underscoring how little we currently understand about the total effect these malicious cyber intrusions have on our economic future.

In addition to the threat posed to our Nation's prosperity, the Counterintelligence Executive's report noted that foreign collectors are stealing information ''on the full array of U.S. military technologies in use or under development,'' including marine systems, aerospace and aeronautics technologies used in intelligence gathering and kinetic operations, such as UAVs, and dual-use technologies used for generating energy.

In April, James Lewis of the Center for Strategic and International Studies testified in an unclassified Senate hearing that the delays and cost overruns in the F–35 program may be the result of cyber espionage, which in turn could be linked to the rapid development of China's J–20 stealth fighter. He went on to note that Iran has also been pursuing the acquisition of cyber attack capabilities, noting that FBI Director Mueller has testified that Iran appears increasingly willing to carry out such attacks against the United States and its allies.

As Director of National Intelligence James Clapper remarked during his unclassified testimony to the Select Committee on Intelligence in January, we are observing an ''increased breadth and sophistication of computer network operations by both state and nonstate actors'' and despite our best efforts ''cyber intruders continue to explore new means to circumvent defensive measures.'' To illustrate this point, Director Clapper cited the well-publicized intrusions into the NASDAQ networks and the breach of computer security firm RSA in March 2011, which led to the exfiltration of data on the algorithms used in its authentication system and, subsequently, access to the systems of a U.S. defense contractor.

Consequently, as Director Clapper put it, one of our greatest strategic challenges in the coming years will be ''providing timely, actionable warning of cyber threats and incidents, such as identifying past or present security breaches, definitively attributing them, and accurately distinguishing between cyber espionage intrusions and potentially disruptive cyber attacks.''

As I listened to Director Clapper's assessment of the cyber threat at the Intelligence Committee's annual unclassified worldwide threat hearing this past January, I was reminded of similar statements by several of his predecessors. In fact, on February 2, 2010, then DNI Dennis Blair provided the following cautionary warning:

> This cyber domain is exponentially expanding our ability to create and share knowledge, but it is also enabling those who would steal, corrupt, harm or destroy the public and private assets vital to our national interests. The recent intrusions reported by Google are a stark reminder of the importance of these cyber assets, and a wake-up call to those who have not taken this problem seriously.

Similarly, the preceding year, on February 12, 2009, Director Blair said:

> Over the past year, cyber exploitation activity has grown more sophisticated, more targeted, and more serious. The Intelligence Community expects these trends to continue in the coming year.

As far back as February 5, 2008, then-DNI Michael McConnell warned:

> It is no longer sufficient for the US Government to discover cyber intrusions in its networks, clean up the damage, and take legal or political steps to deter further intrusions. We must take proactive measures to detect and prevent intrusions from whatever source, as they happen, and before they can do significant damage.

It was in response to this cavalcade of wake-up calls and threat briefings that Senator ROCKEFELLER and I, in our role as crossover members of both the Intelligence and Commerce committees, initiated a series of hearings before the Commerce Committee to begin considering proposals for collaborating with the private sector to prevent and defend against attacks in cyber space.

On April 1, 2009, Senator ROCKEFELLER and I introduced one of the first bills aimed at tackling some of our Nation's most vexing challenges when it comes to this issue. Our legislation, the Cybersecurity Act of 2010, was meant to focus the Senate's efforts on several key priorities, including conducting risk assessments to identify and evaluate cyber threats and vulnerabilities, clarifying the responsibilities of government and private sector stakeholders by creating a public-private information sharing clearinghouse, and investing in cyber research and development to expand activities in critical fields like secure coding, which is indispensable in minimizing our vulnerability to cyber intrusions. Our bill also sought to expand efforts to recruit the next generation of ''cyber warriors'' to implement these defenses through the creation of a cyber scholarship-for-service program.

Our cyber security bill was one of the first attempts to confront our vulnerabilities in cyber space, and with approximately 90 percent of the Nation's digital infrastructure controlled by private industry, we made a concerted effort to collaborate with businesses and ensure our bill incorporated input from experts covering the complete spectrum of this issue. Along the way Senator ROCKEFELLER and I have worked together closely, holding meetings with the White House Cyber Security Coordinator, conducting hearings at the Commerce Committee with experts like James Lewis of the Center for Strategic and International Studies

and former Director of National Intelligence Mike McConnell, and collaborating on a Wall Street Journal op-ed entitled ''Now Is the Time to Prepare for Cyberwar.''

As a result, our legislation was marked up in a unanimous, bipartisan effort by the Commerce Committee in 2010. Moreover, our proposal received praise from a major telecommunications industry leader who said our 2009 bill ''puts the nation on a much stronger footing'' to confront the cyber threat and a leading telecom association, which said that ''passage of the Rockefeller-Snowe Cybersecurity Act is a necessary and important step in protecting our national infrastructure.''

Additionally, in February 2011, following the Egyptian Government's attempt to quell public protests by denying access to the Internet, I pledged to oppose so-called ''Internet kill switch'' authority here in the United States. Consequently, I was pleased when earlier this year Senators on both sides of the aisle joined me in protecting critical first amendment rights by agreeing to reject any provisions that could be construed as giving our government new authority to restrict access to the Internet.

Thus, although I am not a cosponsor of the legislation before the Senate, I recognize that this proposal reflects many of the core ideas first offered by Senator ROCKEFELLER and I in 2009, and I commend my colleagues for working with us over the last few years to ensure that these essential provisions were made part of the revised cyber security legislation.

Specifically, I support steps taken in the revised bill that require collaboration between the government and the private sector to share information about cyber threats and identify vulnerabilities to protect networks. Such information sharing and sector-by-sector cyber risk assessments were a fundamental part of the Rockefeller-Snowe bill in 2009. Likewise, I support provisions establishing an industry-led—rather than government-led—process for identifying best practices, standards, and guidelines to effectively remediate or mitigate cyber risks, with civil liability protection for those owners and operators of critical infrastructure who have implemented these standards. And I support the cyber outreach, awareness, recruitment, and workforce development provisions that were an essential component of our original bill.

That being said, the private sector is rightly concerned about the prospect of over-regulation by the Federal Government. Specifically, many of my colleagues on the Republican side of the aisle have expressed concerns that passage of a comprehensive cyber security bill could lead to more government redtape, stifling innovation and impeding growth.

Yet I firmly believe these are not insurmountable challenges, and I am optimistic that there is tremendous potential for the Senate to forge a viable solution that incentivizes private sector participation and collaboration.

Although the revised bill takes steps to incentivize the adoption of voluntary cyber security practices, many continue to voice concerns when it comes to the provisions governing ''covered critical infrastructure,'' or in other words, those information systems for our transportation, first responders, airports, hospitals, electric utilities, water systems, and financial networks whose disruption would interrupt life-sustaining services, cause catastrophic economic damage, or severely degrade national security.

I support an effort to raise the bar when it comes to cyber security standards for our most critical, life-sustaining systems. Yet in order to pass a bill that has the momentum to become law, we absolutely must find some middle ground with those who have raised valid concerns about the potential of over-regulation by the Federal Government.

For example, I have heard concerns from the private sector that subsection 103(g) of the revised bill may cause confusion and has led many to believe that the voluntary rules will eventually be forced upon companies who may already have strong security practices in place. Specifically, this subsection mandates that all Federal agencies with responsibilities for regulating critical infrastructure must submit an annual report justifying why they have not acted to make the voluntary standards proposed through this legislation mandatory within their jurisdiction. To remove any confusion about the intent of the bill, I am working with Senator WARNER and several of my colleagues on straightforward language to clarify that nothing in the bill should be construed to increase, decrease, or otherwise alter the existing authority of any Federal agency when it comes to the security of critical cyber infrastructure.

Likewise, I share some of my colleagues' concerns that provisions designed to bolster the Department of Homeland Security's role in managing efforts to secure and protect critical infrastructure networks could lead to an unsustainable DHS bureaucracy. Such provisions were not part of the original Rockefeller-Snowe bill, which took a different approach by creating a Senate-confirmed National Cybersecurity Adviser within the Executive Office of the President.

Yet, again, this hurdle is not insurmountable—and I welcome the establishment of the National Cybersecurity Council in the revised bill as an interagency body with members from the Departments of Commerce, Defense, Justice, the Intelligence Community, and other appropriate Federal agencies—in addition to DHS—to assess risks and ensure the primary regulators for each critical system are involved in any final decision.

Furthermore, I remain concerned that the bill lacks specific provisions to assist small businesses in complying with any new cyber security standards adopted by Federal agencies with responsibilities for regulating the security of critical infrastructure. Small businesses remain the primary job creators in this country, responsible for more than two-thirds of all new jobs created. As ranking member of the Senate Committee on Small Business and Entrepreneurship, I have advocated tirelessly for targeted regulatory reform because there is no doubt that regulations are stifling small business. Small firms with fewer than 20 employees bear a disproportionate burden of complying with Federal regulations. These small firms pay an annual regulatory cost of $10,585 per employee, which is 36 percent higher than the regulatory cost facing larger firms.

In response, I have proposed several amendments to ensure the Small Business Administration and other constructive stakeholders are involved in analyzing the implications of cyber security performance standards on small businesses and recommending options for mitigating any costs or unnecessary burdens. And I have filed an amendment that would identify the challenges that prevent the Federal Government from leveraging the capabilities of small businesses to perform classified cyber security work and to develop security-cleared cyber workers.

I have also filed amendments that ensure sector specific regulators have the technical resources and staffing to adequately address cyber threats facing their industry and that focus research efforts on promising technologies that will secure our wireless infrastructure. Additionally, I have joined my colleague, Senator TOOMEY, in offering an amendment that would implement a national data security breach standard to simplify compliance for businesses and notifications to consumers to reduce undue burden and confusion. More than 540 million records have been reported breached since 2005 according to the Privacy Rights Clearinghouse, and research from Symantec estimates the average organizational cost of a breach is approximately $5.5 million.

Finally, I have filed an amendment to prohibit our government from signing new trade agreements with countries that have been identified by the National Counterintelligence Executive as using cyber tools to steal our trade secrets and threaten our economic security. It is time to send the message that these malicious activities will come with a price, and I view this as a sound and practical means of deterrence.

So again let me reiterate the imperative fact that time is not on our side. As former Secretary of Homeland Security Michael Chertoff and several of his intelligence community and defense colleagues recently wrote in a letter to our Senate leadership, the

risk of failing to act on comprehensive cyber security legislation is ''simply too great considering the reality of our interconnected and interdependent world, and the impact that can result from the failure of even one part of the network across a wide range of physical, economic and social systems.''

Therefore, as I wrote in a letter to the majority and minority leaders in June, ''given the nature of the threat we face . . . it is essential that we not miss an opportunity to consider cyber security legislation in a non-partisan manner and pass a bill that has the momentum to become law.''

Now is the moment to prove that the Senate is capable of forging a viable solution to address what Director Clapper called ''a critical national and economic security concern.'' I welcome this debate on what I view as one of the defining national security challenges of our generation, and I urge my colleagues to join me in working for passage of comprehensive cyber security legislation.

Mr. AKAKA. Mr. President, today I wish to urge my colleagues to allow an up-or-down vote on the Cybersecurity Act of 2012, S. 3414, and to support my amendment to further strengthen the privacy safeguards in this important legislation.

National security experts from both parties have warned us about the very serious danger of a major cyber attack. It is not a matter of if, but when it will occur. As someone who witnessed the attack on Pearl Harbor and was in Washington, DC, on September 11, 2001, it is frightening to know that in our modern world where much of our critical infrastructure and security systems are controlled by computers, a successful attack on a critical system could lead to more loss of life, injury, and damage than those terrible events. We have a moral duty to act immediately. That is why I urge my colleagues to put partisan differences aside and pass the Cybersecurity Act of 2012 for the safety of our Nation.

As a senior member of the Senate Homeland Security and Governmental Affairs Committee, I know that Chairman LIEBERMAN and Ranking Member COLLINS have been working diligently for several years to get this bill to the floor for a vote. Commerce Committee Chairman ROCKEFELLER and Intelligence Committee Chairman FEINSTEIN have also been working tirelessly to advance this legislation. While I continue to support the even stronger critical infrastructure protections in the original cyber security bill introduced in February, I accept the revisions the bill sponsors have made to accommodate concerns raised by several of my colleagues.

I want to thank the bill sponsors for working with me during this lengthy process to make improvements to the legislation. In order for our country to have robust cyber security capabilities, we must have a talented and well-trained cyber workforce. I am pleased that the bill incorporates my recommendations to strengthen title IV of the bill, which provide the necessary tools to build a first-class cyber workforce while maintaining employee and whistleblower protections. Furthermore, these workforce provisions establish a supervisory training program that will help managers properly evaluate their cyber employees.

I also want to commend the sponsors for the marked improvement of the underlying privacy and civil liberties protections in the bill. I collaborated with Senators FRANKEN, DURBIN, WYDEN, SANDERS, COONS, and BLUMENTHAL to strengthen protections in the information-sharing provisions of the bill, which allow companies to share cyber security information with each other and the government. We worked with privacy and civil liberties groups from across the political spectrum on a series of recommendations, most of which were accepted by the bill's sponsors.

With these changes, the privacy and civil liberties protections in the Cybersecurity Act are much better than the protections contained in the Cyber Intelligence Sharing and Protection Act that recently passed the House, and the SECURE IT Act that has been introduced in the Senate. However, I am still pushing for further improvements to enhance the privacy and civil liberties protections in the Cybersecurity Act.

I have offered an amendment that seeks to strengthen the underlying legal framework protecting Americans' personal information held in the computer systems that the Cybersecurity Act seeks to protect. My amendment will close loopholes in Federal privacy requirements, centralize Federal oversight of existing privacy protections, and reinstate basic remedies for privacy violations. My amendment, which reflects input from the bill's sponsors, would make four small changes that would have significant benefits to American's privacy and data security.

First, my amendment would address Federal agencies' uneven implementation of Office of Management Budget, OMB, guidance on preventing breaches of private information and notifying affected individuals when they do occur. In testimony this week before the Oversight of Government Management Subcommittee that I chair, we learned that the agency that oversees the Thrift Savings Plan, TSP, had no breach notification plan in place at the time of the recent breach involving 123,000 participating Federal employees. Specifically, my amendment would strengthen data breach notification requirements for Federal agencies by directing OMB to establish requirements for agencies to provide timely notification to individuals whose personal information was compromised. It would require agency heads to comply with the policies, and mandate that OMB report to Congress annually on agencies' compliance.

Second, my amendment would provide basic transparency when agencies rely on commercial databases. Agencies frequently use private sector databases for law enforcement and other purposes that affect individuals' rights, but this is not covered by Federal privacy laws. My amendment would require agencies to conduct privacy impact assessments on agencies' use of commercial sources of Americans' private information so that individuals have appropriate protections such as access, notice, correction, and purpose limitations.

Third, my amendment would fill a hole in the government's privacy leadership. Despite OMB's mandate to oversee privacy policies government-wide, it lacks a chief privacy officer. As a result, responsibility for protecting privacy is fragmented and agencies' compliance with privacy-related statutes and regulations is inconsistent. Furthermore, the administration lacks a representative on international privacy issues. My amendment would direct OMB to designate a central officer within OMB who would have authority over privacy across the government. This officer would also be responsible for assessing the privacy impact of the new information-sharing provisions in the cyber security bill.

Finally, it would address the Supreme Court's ruling restricting Privacy Act remedies earlier this year that has by many experts' accounts rendered the Privacy Act toothless. In Federal Aviation Administration v. Cooper, the Social Security Administration violated the Privacy Act by sharing the plaintiff's HIV status with other Federal agencies. The Court concluded that the plaintiff could not recover damages for emotional distress because Privacy Act damages are limited to economic harm. My amendment would heed the call of scholars across the political spectrum to amend the Privacy Act and fix this decision. It would also clarify that in the event of a Federal violation in the information-sharing title of the bill, a victim would be entitled to recovery for the same types of noneconomic harms.

My amendment will further strengthen the privacy and civil liberties protections in the cyber security bill while enhancing the security of personal information held by the Federal Government. I urge my colleagues to allow an up-or-down vote on the Cybersecurity Act, which is so critical to our Nation's safety, and to support my amendment.

Mr. LEAHY. Mr. President, today, the Senate will conclude debate on the Cybersecurity Act of 2012, S. 3414. Developing a comprehensive strategy for cybersecurity is one of the most pressing challenges facing our Nation. I commend President Obama for his commitment to addressing this national security issue. I also commend the majority leader and the bill's sponsors for their work on this pressing matter.

I share the President's view that updates to our laws are urgently needed

to keep pace with the many threats that Americans face in cyberspace. For that reason, I will support the motion for cloture on this bill. But, I do so with major reservations about the bill in its current form because this legislation does not address many of the key priories that must be a part of our national strategy for cybersecurity.

A legislative response to the growing threat of cyber crime must be a part of our debate about cyber security. Protecting American consumers and businesses from cyber crime and other threats in cyber space is a top priority of the Judiciary Committee. That is why I filed an amendment to the bill to strengthen our Nation's cyber crime laws, which takes several important steps to combat cyber crime. The amendment, among other things, updates the Federal RICO statute to add violations of the Computer Fraud and Abuse Act to the definition of racketeering activity; strengthens the legal tools available to law enforcement to protect our Nation's critical infrastructure by making it a felony to damage a computer that manages or controls national defense or other critical infrastructure information; and streamlines and enhances the penalty structure under the Computer Fraud and Abuse Act. This cyber crime amendment incorporates many of the proposals that were recommended in the cyber security proposal that President Obama delivered to Congress last May. The Judiciary Committee favorably reported these proposals in September as part of my Personal Data Privacy and Security Act. These updates to our criminal laws are urgently needed to keep pace with the cunning of cyber thieves and the many emerging threats to American's safety in cyber space. These measures must be included in any cyber security legislation the Senate considers.

In the digital age, we must also update our digital privacy laws so that Americans will have better safeguards for their electronic communications. That is why I filed an amendment to the bill that makes commonsense updates to two vital digital privacy laws that I authored several years ago—the Video Privacy Protection Act, VPPA, and the Electronic Communications Privacy Act, ECPA. The amendment would update the Video Privacy Protection Act to permit consumers to provide a one-time consent for video service providers to share their video viewing information with third parties via the Internet. This update will help the VPPA keep pace with how most Americans view and share videos today—on the Internet—while also requiring that video service providers provide clear and conspicuous notice that the consent to share video viewing information can be withdrawn at anytime. The amendment also updates the Electronic Communications Privacy Act to prohibit service providers from voluntarily disclosing the contents of Americans' e-mails or other electronic communications to the Government, unless the Government obtains a search warrant based on probable cause. There are appropriate exceptions to this prohibition under current law, including when a customer provides consent or when disclosure to law enforcement is necessary to address certain criminal activity. I am also mindful of the need to ensure that law enforcement can do their jobs effectively. The safeguards and exceptions in this provision were designed to ensure that appropriate privacy protections do not undermine the ability of law enforcement to keep us safe.

I also filed a bipartisan amendment to promote cyber research and development in Vermont and elsewhere across the Nation. This amendment improves section 301 of the bill by clarifying that the White House's Office of Science and Technology Policy's new test bed program should build upon existing work on cybersecurity test beds by the Department of Homeland Security in its Science and Technology Directorate. The amendment also expands the proposed test beds program to include funding for the military academies and senior military colleges to participate. Senator HOEVEN joined me in proposing this improvement to the bill, and we both believe that it is important for these institutions, which have such a prominent role in cultivating the next generation of security leaders, to develop tools to combat the next generation's security threats.

Comprehensive cyber security legislation must also respond to the alarming number of data security breaches that threaten the privacy and security of American consumers and businesses today. The troubling data breaches at Sony, Epsilon, and Lockheed are recent reminders that new tools are needed to protect us from the growing threats of data breaches and identity theft. In May 2011, the Obama administration submitted a data breach proposal that adopted the carefully balanced framework of data privacy and security legislation that I have introduced—and that this Judiciary Committee has favorably reported—several times. My data breach amendment would establish a single nationwide standard for data breach notification. My data security amendment would require that companies that maintain databases with Americans' sensitive personal information establish and implement data privacy and security programs, so that data breaches do not occur in the first place. I filed these amendments because Congress must address the threat of data security breaches and make these long overdue privacy protections available to American consumers and businesses.

The threats to our privacy and security in cyber space are real, and these threats will not go away simply because the Congress fails to act. I lament the fact that a long-overdue debate on cybersecurity legislation has become embroiled in a partisan stalemate. While there are legitimate differences on how we must confront this threat, Democrats, Republicans, and Independents alike are put at risk if we do not do so. We must find a way to work together to confront this national challenge. I hope we will see more progress on overcoming differences on this issue in the weeks ahead. I also hope the sponsors of this bill will include the priorities I have outlined as part of any future comprehensive cyber security bill. Again, I commend the President and all Senators on both sides of the aisle who have worked to address this important issue. I also thank the many privacy, civil liberties, and technology organizations that have supported my amendments to this bill.

I ask that a copy of three letters I have received in support of several of my amendments to the bill be printed in the RECORD following my full remarks.

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

Hon. HARRY REID,
Senate Majority Leader.
Hon. MITCH MCCONNELL,
Senate Minority Leader.

DEAR LEADER REID AND LEADER MCCONNELL: as the Senate considers cybersecurity legislation, we urge you to make in order and to support an amendment that Chairman Leahy has introduced that would update a key privacy law that is critical to business, government investigators and ordinary citizens.

Chairman Leahy's amendment #2580 addresses the Electronic Communications Privacy Act (ECPA), a law that Chairman Leahy himself wrote and guided through the Senate in 1986. ECPA was a forward-looking statute when enacted. However, technology has advanced dramatically since 1986, and ECPA has been outpaced.

As a result, ECPA is a patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty for service providers, for law enforcement agencies, and for the hundreds of millions of Americans who use mobile phones and the Internet. Moreover, the Sixth Circuit Court of Appeals has held that a provision of ECPA is unconstitutional because it allows the government to compel a service provider to disclose the content of private communications without a warrant.

Chairman Leahy's amendment would make it clear that, except in emergencies, or under other existing exceptions, the government must use a warrant in order to compel a service provider to disclose the content of emails, texts or other private material stored by the service provider on behalf of its users.

Chairman Leahy's amendment would create a more level playing field for technology. It would cure the constitutional defect identified by the Sixth Circuit. It would provide clarity and certainty to law enforcement agencies at all levels, to business and entrepreneurs, and to individuals who rely on online services to create, communicate and store personal and proprietary data. These protections for content are consistent with an ECPA reform principle advanced by the Digital Due Process coalition, www.digitaldueprocess.org, a broad-based coalition of companies, privacy groups, think tanks, and academics.

For Internet and communications companies competing in a global marketplace, and

for citizens who have woven these technologies into their daily lives, as well as for government agencies that rely on electronic evidence, the protections for content in the Leahy amendment would represent an important step forward for privacy protection and legal clarity.

While the signatories to this letter have very diverse views on the cybersecurity legislation, and some take no position on the legislation, we urge you to make the Leahy amendment #2580 in order and to support it when offered.

Sincerely,

Adobe; American Booksellers Foundation for Free Expression; Americans for Tax Reform; Association for Competitive Technology; American Library Association; Association of Research Libraries; Bill of Rights Defense Committee; Business Software Alliance; CAUCE North America; Center for Democracy & Technology; Center for Financial Privacy and Human Rights; Center for National Security Studies; Citizens Against Government Waste; Competitive Enterprise Institute; Computer and Communications Industry Association; The Constitution Project; Data Foundry; Distributed Computing Industry Association; eBay; EDUCAUSE; Engine Advocacy; FreedomWorks; Liberty Coalition; Newspaper Association of America; Microsoft; Neustar; Personal; Salesforce; Sonic.net; SpiderOak; Symantec; TechFreedom; TechAmerica; TRUSTe; U.S. Policy Council of the Association for Computing Machinery.

SEPTEMBER 21, 2011.

Hon. PATRICK LEAHY,
Chairman, Committee on the Judiciary, U.S. Senate, Washington, DC.
Hon. CHARLES GRASSLEY,
Ranking Member, Committee on the Judiciary, U.S. Senate, Washington, DC.

DEAR SENATORS LEAHY AND GRASSLEY: The undersigned individuals and organizations wrote last month in support of making changes to the Computer Fraud and Abuse Act to ensure that it is both strong and properly focused. We mentioned that while the CFAA is an important tool in the fight against cybercrime, its current language is both overbroad and vague. It can be read to encompass not only the hackers and identity thieves the law was intended to cover, but also actors who have not engaged in any activity that can or should be considered a ''computer crime.'' We write again today to express our appreciation for recent action taken by the Committee on the Judiciary to address our concerns.

Last week, at a markup of Chairman Leahy's Personal Data Privacy and Security Act of 2011 (S. 1151), Senator Grassley, with the co-sponsorship of Senators Franken and Lee, introduced an amendment that would fix a large part of the overbreadth problem in the CFAA. In particular, the amendment would remove the possibility that the statute could be interpreted to allow felony prosecutions of ''access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized.'' The amendment passed with bipartisan support, including that of Chairman Leahy himself.

As we noted in our previous letter, our concerns about overbroad interpretations of the existing language are far from hypothetical. Three federal circuit courts have agreed that an employee who exceeds an employer's network acceptable use policies can be prosecuted under the CFAA. At least one federal prosecutor has brought criminal charges against a user of a social network who signed up under a pseudonym in violation of terms of service.

These activities should not be ''computer crimes'' any more than they are crimes in the physical world. If, for example, an employee photocopies an employer's document to give to a friend without that employer's permission, there is no federal crime (though there may be, for example, a contractual violation). However, if an employee emails that document, there may be a CFAA violation. If a person assumes a fictitious identity at a party, there is no federal crime. Yet if they assume that imaginary identity on a social network that prohibits pseudonyms, there may again be a CFAA violation. This is a gross misuse of federal criminal law. The CFAA should focus on malicious hacking and identity theft and not on criminalizing any behavior that happens to take place online in violation of terms of service or an acceptable use policy.

We believe that the Grassley/Franken/Lee amendment is an important step forward for both security and civil liberties. We commend the Ranking Member for introducing the amendment and the Chairman for supporting it. We would also support further changes to the language in the bill to ensure that government employees are given the same protections from criminal prosecution as their private sector counterparts. Changes such as these will strengthen the law and focus the justice system on the malicious hackers and online criminals who invade others' computers and networks to steal sensitive information and undermine the privacy of those whose information is stolen.

Sincerely,

Laura W. Murphy, Director, Washington Legislative Office, American Civil Liberties Union; Kelly William Cobb, Executive Director, Americans for Tax Reform's Digital Liberty; Leslie Harris, President and CEO, Center for Democracy & Technology; Fred L. Smith, President, Competitive Enterprise Institute; Marcia Hofmann, Senior Staff Attorney, Electronic Frontier Foundation; Charles H. Kennedy, Partner, Wilkinson, Barker, Knauer, LLP; Wayne T. Brough, Ph.D., Chief Economist and Vice President, Research, FreedomWorks Foundation; Orin S. Kerr, Professor of Law, George Washington University; Paul Rosenzweig, Visiting Fellow, The Heritage Foundation; Berin Szoka, President, TechFreedom.

TECHAMERICA,
Washington, DC, July 30 2012.

Re U.S. Senate Proposed Cybersecurity Legislation

Hon. HARRY REID,
Majority Leader, U.S. Senate, Washington, DC.
Hon. MITCH A. MCCONNELL,
Minority Leader, U.S. Senate, Washington, DC.

DEAR MAJORITY LEADER REID AND MINORITY LEADER MCCONNELL: On behalf of TechAmerica, thank you for your leadership in making cybersecurity a national priority. We share your goal of enhancing our nation's cybersecurity posture in response to growing cyber threats. TechAmerica believes that any final bi-partisan agreement should both preserve the vitality of innovation and promote the Information & Communication Technology sector's ability to respond to constantly evolving cyber threats. With these goals in mind, we are writing to provide our insights on S. 3414, the Cybersecurity Act of 2012, and additional elements for the Senate's consideration as part of a final cybersecurity package designed to help meet our national security challenges.

TechAmerica and its members are dedicated to maintaining and expanding the partnership between the private sector and the government to address our nation's cybersecurity preparedness. We have spent much time over the last six years focusing on these critical issues, working closely with Congress and the Administration on addressing threats to our nation's cybersecurity. Any final cybersecurity measure passed by the Senate must be firmly grounded in a strong public private partnership.

We believe that legislation, if not done carefully, could do more harm than good. Specific mandates generally do not adapt as quickly as threat and technology landscapes change, so they can actually hinder industry's ability to innovate and effectively mitigate threats. Mandates affect industry's ability to design, develop and deploy technology. S. 3414 represents a clear step forward towards a workable framework that strikes the right balance by prioritizing our nation's cybersecurity with an outcome based approach of voluntary incentives rather than through prescriptive regulatory mandates.

As the Senate prepares to consider S. 3414, The Cybersecurity Act of 2012, as the underlying bill to comprehensive cybersecurity legislation, we wish to convey our strong support of several critical components that would immediately enhance our cybersecurity posture. Specifically, TechAmerica endorses the following provisions of S. 3414 to address our country's critical cybesecurity priorities:

Title—Federal Information Security Management Act (FISMA) Reform: The paper-based, compliance regime that exists under the current FISMA framework is time consuming and costly. This outdated system has not demonstrated a requisite increase in security of government systems. In response to a rapidly evolving threat environment, our federal information security practices must be updated to reflect a risk-based and continuous monitoring approach as proposed by Senator Carper in Title II of S. 3414.

Title III—Research and Development: Investing in research and development (R&D) is essential to protecting critical systems and enhancing the cybersecurity for both the government and the private sector. We support Title II, which would create a national cybersecurity R&D plan to help develop game-changing technologies that will neutralize attacks on the cyber systems of today and lay the foundation to meet the challenges of securing the cyber systems of tomorrow.

Title IV—Education, Workforce, and Awareness: Industry and government must work together to plan for the future by investing in cybersecurity education to develop the next generation of cybersecurity workers. We support Title IV, which encourages cybersecurity professional development and improving public awareness of cybersecurity risks from identity theft to cyber predators and fraudsters.

Title V—Federal Acquistion Risk Management Strategy: We support Title V, which calls for a comprehensive acquisition risk management strategy to address risks and threats to the information technology products and services in the federal government supply chain. This strategy will allow agencies to make informed decisions when purchasing IT products and services. Importantly, the bill requires specific and much needed training for the federal acquisition workforce to enhance the security of federal networks.

Title VI—International Cooperation: Cybercrimes are borderless, and we must work with our international partners to combat this threat. Title VI will help provide for enhanced cyber response capacity in countries currently without adequate resources to combat cybercrime, as well as use

of existing legal mechanisms to further international cooperation. We support Title VI, which includes S. 1469, The International Cybercrime Reporting and Cooperation Act, sponsored by Senators Hatch and Gillibrand.

TechAmerica is confident that these core components alone would immediately and substantially improve America's cybersecurity posture. Congress cannot afford to delay any longer on the passage of these critical provisions considering the potential risk of falling behind our cyber adversaries.

In an effort to provide the Senate with our collective expertise, we are also compelled to outline for you those aspects of the legislation that we believe require further refinement in order for it to receive our overall support as a final cybersecurity proposal. These provisions include:

Title I—Public Private Partnership to Protect Critical Infrastructure: Rather than mandating that critical infrastructure organizations comply with a DHS cybersecurity framework, the newly introduced bill offers a vast, important improvement by providing incentives to organizations that voluntarily comply with cybersecurity best practices. While we commend this positive direction, TechAmerica recommends further refining the following provisions of Title I.

National Cybersecurity Council—In the spirit of a true public-private partnership, industry should be represented by the Sector Coordinating Councils (SCCs) in an official capacity on the National Cybersecurity Council. Best practices and voluntary standards should be industry driven and developed in conjunction with NIST. The Council should not have the ability to unilaterally overrule the SCCs proposed best practices. Alternatively, we therefore propose a conciliatory dispute resolution process.

Inventory of Critical Infrastructure—We recommend that each sector be differentiated and recognized for current cybersecurity best practices employed in securing critical infrastructure. Information technology is not only a specific sector, but an underlying component of multiple industry sectors. For this reason, we strongly support preserving the current back-end limitation on commercial information technology products.

Voluntary Cybersecurity Best Practices—We urge the sponsors to strike any reference to the term ''mandatory'' in the text to ensure this framework is truly voluntary in nature and not a precursor to future regulatory action.

Voluntary Cybersecurity Program for Critical Infrastructure—TechAmerica requests inserting liability protection language that will prevent compensatory damages, a cap on damages for vicarious liability, and bar punitive damages.

Protection of Information—While we strongly support the protection of information found in Section 106, we are concerned by some of the additional, extraneous mechanisms introduced as part of that protection. Such elements of the proposal act as a clear disincentive to private companies joining a voluntary system in good faith out of concern for future audit and investigation.

Title VII—Information Sharing: The inability to share information is one of the greatest challenges to collective efforts toward improving our cybersecurity, and we appreciate the efforts by the sponsors of S. 3414 to remove those barriers in order to foster better information sharing between the government and the private sector. We believe that information sharing is a fundamental component of S. 3414, as it will better enable collaboration in defense of cyber-attacks while ensuring strong privacy protections. TechAmerica recommends refining the following provisions of S. 3414 in Title VII.

Affirmative Authority to Monitor and Defend Against Cybersecurity Threats—S. 3414 significantly narrows the scope of ''monitoring'' activities permissible under previous bill iterations to the scrutiny of a specific list of ''cyber threat indicators.'' Previously proposed language had allowed companies to monitor for cybersecurity threats, which were defined more generally as unauthorized access or exfiltration, manipulation, or impairment to the network or data. It isn't clear that industry's standard monitoring systems can be tailored enough to fit within the parameters of the more specific list as some threats are not categorized until after they are detected through system alerts. In addition, Title VII in its current form limits how an entity may use cyber threat information that it obtains from its own monitoring. This is a significant limitation to put on entities and does not seem justified. The laundry list approach used to define cyber threat indicators potentially limits the use of some techniques tailored to protect networks. It is problematic that this definition is linked to monitoring authority. Finally, we believe that the definition of countermeasures should be narrowed.

Voluntary Disclosure of Cybersecurity Threat Indicators Among Private Entities—Business to business information sharing is an important practice in preventing cyber threats. We recommend striking the reasonably likely standard provision in this Title. It is a difficult test to meet and one that will only discourage private information sharing. Also, we believe that more business to business information sharing would be possible with the inclusion of the same limited liability protection that a private entity would receive when sharing information with the newly created government exchange.

In closing, TechAmerica urges the Senate to act on and pass the following legislative measures which may possibly be offered as amendments to S. 3414, The Cybersecurity Act of 2012:

Cybercrime: TechAmerica urges the Senate to pass S. 2111, The Cyber Crime Protection Security Act, sponsored by Senator Leahy. This measure will provide the government with new tools to prosecute more effectively organized criminal activity involving computer fraud. The legislation will also streamline and enhance the criminal penalties for computer fraud, and address cybercrime involving the trafficking of consumers' online passwords.

Electronic Communications Privacy: TechAmerica supports, S. 1011, The Electronic Communications Privacy Amendments Act, sponsored by Senator Leahy which would update the 1986 ECPA statute to give information stored in the cloud the same level of protection afforded to information stored locally.

Data Breach Notification: TechAmerica has long supported passage of a strong, national data breach notification law and has endorsed S. 1207, the Data Security and Breach Notification Act, sponsored by Senators Rockefeller and Pryor as the approach consistent with our principles on data breach notification. Establishing a national framework to promote on-going data security measures and consistent breach notification standards will provide much needed guidance, predictability, and certainty for consumers, consumer protection authorities, and businesses, and will replace the complex patchwork of state data breach laws with a uniform national standard.

As you and your colleagues attempt to find bi-partisan consensus on a final cybersecurity agreement, we urge you to carefully consider sustaining the innovative capacity of our information and communications systems and all the myriad activities that they enable, and to thus observe the important axiom, ''first, do no harm.'' Cybersecurity is a multi-faceted and complex ecosystem with profound interdependencies; thus even well intended legislation in this area often has the potential to produce many unintended consequences. Without such rigorous review and consultation, legislation could possibly potentially violate this cardinal principle and risk setting us back in our collective efforts to bolster our nation's cybersecurity.

Thank you again for considering our views and for your continued efforts to enhance our nation's cybersecurity. As representatives of the nation's leading information and communications technology firms, TechAmerica remains strong in our resolve to continue working together with the Senate and the House to improve the security of our shared cyberspace.

Sincerely,

SHAWN OSBOURNE,
President and CEO.

Mr. MCCAIN. Mr. President, I rise today to oppose cloture on the Cybersecurity Act of 2012.

Are any of us surprised that we find ourselves in this situation—again? Is this the ''open amendment'' process we were all promised? As I said earlier this year, a bill as complex as cyber security legislation can only be achieved if it goes through the regular committee process. Had this bill been subjected to the proper committee process, instead of relying on Senate rule XIV, I believe we would have had a much stronger legislative product that would have attracted broader support. Instead, the blame game, which is the first sign of a stalled legislative process, is in full swing.

As of yesterday afternoon it was my understanding that we would continue to work throughout August to find a compromise on this legislation. As a backstop to prepare for the possibility that an agreement would not be reached during that time, we requested a tranche of 10 to 15 placeholder amendments be set aside to address a defined set of issue areas we had with the current bill. In exchange for these process concessions, our group was willing to support cloture.

The unfortunate reality is that we had time to conduct proper legislative hearings and hold committee markups. But rather than choose the customary process, which forces us to defend our points of view, build consensus around ideas and, admittedly, requires more planning and hard work, a less transparent approach was taken. That approach, while at the time may have seemed more legislatively convenient, resulted in hurried, last-minute negotiations that have been doomed from the outset. Rarely does anything good get accomplished under these circumstances, which lack transparency and scrutiny. This should serve as a warning to both sides of the aisle and future congresses that attempts to side-step the legislative process are risky, often unproductive, and do not bypass the criticism they seek to avoid.

And while all of us recognize the importance of cyber security, we should

not confuse opposition to this deeply flawed bill as a sign of somehow being unwilling to address the issue. It has been my experience that when dealing with matters of national security and domestic policy, and in this bill is at the nexus of both, it is more important to work to get something done right than just work to get something done. And while both efforts may result in enough material to create a headline, only one fulfills our purpose for being here in this body.

Time and again, we have heard from experts about the importance of maximizing our Nation's ability to effectively prevent and respond to cyber threats. We have all listened to these accounts. This cyber threat and the risk of an attack only increased when the Stuxnet leaks began recklessly coming out of this administration. And while this threat and others persist, the most important piece of legislation which the congress can pass when it comes to ensuring our national security, the National Defense Authorization Act, which includes cyber security elements, remains unfinished. This entire process feels more like a ploy to advance the fiction that we are focused on national security, while avoiding the fulfillment of one of the Congress's most important national security responsibilities—the passage of the National Defense Authorization Act.

The point is that debating a controversial and flawed bill—a bill of such 'significance' that it has languished for over 5 months at the Homeland Security and Government Affairs Committee, with no committee markup or normal committee process—should not have taken precedence over a bill which was vetted over a period of 4 months by the Senate Armed Services Committee and reported to the floor with the unanimous support of all 26 members. Unfortunately, our current trajectory will likely leave us without a cyber security bill or the National Defense Authorization Act.

As I have said time and time again, the threat we face in the cyber domain is among the most significant and challenging threats of 21st-century warfare. But this bill unfortunately takes us in the wrong direction and establishes a new national security precedent which fails to recognize the gravity of the threats we face in cyber space. I agree that we must take appropriate steps to ensure that civil liberties are protected and believe we could have appropriately done so without removing the only institutions capable of protecting the United States from a cyber attack from counties like China, Russia, and Iran—from the front lines. Making these entities more reliant on their less capable civilian counterparts is an unacceptable, precedent setting approach, which fails to recognize the unique real-time requirements for understanding the threat environment, anticipating attacks, and responding when necessary.

Additionally, what is not being discussed enough are the likely implications of the new cyber security stovepipes being proposed in this bill. The recreation of the very walls and information sharing barriers that the 9/11 Commission attributed as being responsible for one of our greatest intelligence failures is very unwise.

In addition to the problems with the information sharing provisions, the critical infrastructure language grants too much authority to the government, failing to consider the innovative potential of the private sector. I continue to believe that this title would force those who own or operate critical assets to place more emphasis on compliance attorneys, rather than utilize the world-class engineering capabilities employed by our private sector. This is why the primary objective of our bill is to enter into a cooperative information sharing relationship with the private sector, rather than an adversarial relationship rooted in mandates used to dictate technological solutions to industry.

The SECURE IT Act is a serious response to the growing cyber threat facing our country, and it is an alternative approach to the overly bureaucratic and regulatory bill before us. Our amendment seeks to utilize the world-class engineers employed by our private sector, not compliance attorneys in law firms. This is why the primary objective of our bill is to enter into a cooperative information-sharing relationship with the private sector, rather than an adversarial relationship rooted in mandates used to dictate technological solutions to industry.

The centerpiece of the SECURE IT Act continues to be a legal framework to provide for voluntary information sharing. Our amendment provides specific authorities relating to the voluntary sharing of cyber threat information among private entities and the government, and in doing so, we do not create any new bureaucracy. This bill at the very least deserved a vote.

As I stated earlier, it has been my experience that when dealing with matters of national security and domestic policy, it is more important to work to get something done right than just work to get something done. For these reasons, and because of the closed process put forth by the majority, we should all oppose cloture.

Mr. REID. Mr. President, nearly 3 years ago, I called the chairmen of the Senate's national security committees—Senators LIEBERMAN, ROCKEFELLER, FEINSTEIN, LEAHY, and LEVIN—together to discuss what, even then, was one of the most urgent priorities for our national security: defending our Nation against cyber attack.

I asked them to begin working together, across committee jurisdictions and across party lines, to develop comprehensive cyber security legislation to protect our Nation, our security, and our economy from this growing threat. Many of the Senators present had already begun work on their own legislation, but they committed that day to join their efforts in common cause.

Since that time, their committees have painstakingly worked to break down artificial jurisdictional boundaries and to resolve differences across party lines. They have also sought to include a remarkably wide array of stakeholders—including cybersecurity experts, the private sector, academia, the intelligence community, military leaders, law enforcement, think tanks, State and local governments, and many more—in an open, transparent, and cooperative process.

The process has been nearly unprecedented in its scope, its thoroughness, and its transparency. Since the Senate began its work on cyber security legislation in 2009, committees have held more than 20 hearings across at least seven different committees specifically on cyber security and related legislation, and addressed critical questions relating to cyber security in dozens of additional hearings. They have held numerous briefings for Senators and staff on cyber security, including a simulated cyberattack exercise for all Senators conducted by senior administration officials. They have organized several other forums for Senators to examine cyber security issues, including cross-committee working groups designed to develop comprehensive legislation, as well as the Intelligence Committee's 2010 Cyber Security Task Force. They have considered nearly 20 separate cyber security bills and numerous cyber security-related amendments. And they have held markups of cyber security legislation in five separate committees, each of which occurred under each committee's rules for regular order.

The result has been legislation that addresses the equities of these diverse stakeholders as fairly and thoroughly as one could imagine, while preserving the authorities necessary to boost our Nation's cyber defenses.

As ranking member of the Homeland Security Committee, Senator COLLINS has been heroic in her efforts to ensure the bipartisan nature of this process. Yet, despite her best efforts, Republicans have made it clear throughout the last 3 years that they were simply unwilling to participate.

They refused to participate in working groups designed to draft the legislation, despite the fact that these groups were established with Leader MCCONNELL's full agreement. They refused to propose changes to draft legislation, or to participate in negotiations with bill sponsors. When, after 3 years of painstaking work and broad outreach the legislation came to the floor, my Republican colleagues refused to allow the Senate to consider a single amendment to improve the bill, despite my continuous pleading for their agreement on a list of amendments for consideration. And, as today's cloture vote has demonstrated, they have refused to allow us to continue to debate the legislation.

Why this obstinate refusal to participate? How can these Senators, who have received the same entreaties from our military and intelligence leaders about the urgency of this legislation, obstruct Senate action to confront one of the leading threats to our Nation? These questions are all the more perplexing when one considers what our national security leaders have said about the seriousness of the threat we face.

According to General Keith Alexander, Commander of U.S. Cyber Command, ''The cyber threat facing the Nation is real and demands immediate action. The time to act is now; we simply cannot avoid further delay.''

General Martin Dempsey, Chairman of the Joint Chiefs of Staff, noted, ''The uncomfortable reality of our world today is that bits and bytes can be as threatening as bullets and bombs. Not only will military systems be targeted by tools that can cause physical destruction, but adversaries will increasingly attempt to hold our Nation's core critical infrastructure at risk.''

Similarly, Secretary of Defense Leon Panetta stated, ''We talk about nuclear. We talk about conventional warfare. We don't spend enough time talking about the threat of cyberwar. There's a strong likelihood that the next Pearl Harbor that we confront could very well be a cyberattack.''

And Director of National Intelligence James Clapper called cyberattack ''A profound threat to this country, to its future, its economy and its very being.''

Simply put, there is unanimity across the national security community that malicious cyber activity is an urgent, growing, and imminently dangerous threat that our Nation must confront immediately. But this unanimity is not limited to the current administration. Countless national security officials appointed under Republican administrations—including former Director of National Intelligence Mike McConnell, former Secretary of Homeland Security Michael Chertoff, former Deputy Secretary of Defense Paul Wolfowitz, former Chairman of the Joint Chiefs of Staff Mike Mullen, former Director of the Central Intelligence Agency Michael Hayden, and many others—have echoed the urgency of our current administration's call for action, as well as their support for the legislation we have considered today.

Yet, today Republicans were nearly unanimous in their opposition to this legislation. Why?

It is no secret that Republicans are taking their marching orders from the Chamber of Commerce. And the Chamber has made no secret that it is opposed to any effort to secure America's cyber networks; in fact, it has gone so far as to oppose even voluntary cybersecurity standards. In other words, the position of the Chamber of Commerce is that the owners and operators of the most critical infrastructure of our Nation—the electricity grid, telecommunications lines, air traffic control systems, and the like—should not even be asked to take steps, on a strictly voluntary basis, to improve our Nation's security. That position is hard to believe, and it is seriously out of step with the patriotism of the owners and employees of the American businesses it claims to represent.

As a result, my Republican colleagues have ignored the urgent calls of some of America's most respected national security leaders in order to pander to the Chamber of Commerce—an organization that appears more concerned with corporate bottom lines than with the American lives this legislation seeks to defend.

It seems that the only people who have not yet awakened to the threat facing our Nation are Senate Republicans. What has become clear in this debate is that Republicans are willing to prioritize partisan politics and slavish defense of corporate interests over our Nation's security. And that is simply unacceptable.

I hope that my colleagues across the aisle will wake up and recognize the threat facing our country before it is too late—before the ''cyber 9/11'' of which leaders like Secretary Panetta have warned us arrives. I hope that they can join us, as we have asked them to do for the last 3 years, and work on a bipartisan basis for the good of our country. And if they choose to do so, we will be ready to work quickly to pass this much-needed legislation.

But the more they delay, the more the risk to our Nation's security and economy grows. Time is running short.

The ACTING PRESIDENT pro tempore. The Senator from Connecticut is recognized.

Mr. LIEBERMAN. Mr. President, I rise to speak on the vote we will have in about 10 minutes. I am going to be real personal in my statement.

This is one of those days when I fear for our country, and I am not proud of the Senate. We have a crisis, one we all acknowledge. It is not just that there is a theoretical or speculative threat of cyber attack against our country—it is real and happening now. Most people don't know it because a lot of people who are attacked don't want to announce it because they are embarrassed.

A lot of companies are attacked that control critical cyber infrastructure and have, in fact, what I called yesterday secret cyber attack cells planted in their system to control the kind of systems we depend on for the quality of our life and, in some ways, for our lives.

GEN Keith Alexander, Director of Cyber Command at the Pentagon, said the other day that when it comes to cyber war, we are today where we were in 1993 in our war with Islamist terrorism after they blew up the truck bomb in the parking garage at the World Trade Center. We were attacked. It shook us up for a while, but then people forgot about it. At least in that case we knew we had been attacked. Now we are attacked every day and most people don't know it. Maybe there is a story in the paper one day and they read it and it is on TV and then they forget about it.

Are we going to act before we get to the cyber 9/11, as we obviously did in the attacks in a war we were in without acknowledging it with Islamist terrorism? We pretty much all agree on that. Yet we have descended once again to gridlock, to partisan attack and counterattack. The end result of that is a lot of sound and fury that will accomplish nothing, and we will leave our country vulnerable.

The fact is that as the majority leader announced earlier in the week, we have been on this for a long time. Senator COLLINS and I have tried to be flexible. We have been open to compromise, not of principle and how much we thought we could get passed through the Senate, but because the threat is so urgent, we cannot afford to insist on everything we thought was in our best interest. We made a mandatory system voluntary, but that has not been enough. Senator REID said if there was an agreement on a finite list of amendments, and they are germane and relevant to the bill—not taking your favorite political shot through the bill or a political message opportunity—then he would take it up in September. As soon as we come back, we would have limited time on it and go to final passage and the Senate would work its will.

Unfortunately, we haven't been able to agree on such a list. There are still nongermane, irrelevant amendments on the list. Our friends in the Republican caucus have whittled the list down to 58. Frankly, I don't worry about the number as much as the majority leader was right that this bill and the threat of cyber attack and cyber theft is too important to use as a vehicle for political shots at one another.

We are approaching a cloture vote, and now it looks like it is going to lose. I hope not. Hope springs eternal for at least 25 minutes more. I say to my friends, if they believe we are in a cyber war and we are inadequately defended—particularly the part of our cyber infrastructure controlled by the private sector—then vote for cloture. It is the only way we are going to get to this bill. Vote for cloture.

Remember something. We are just one of two Chambers of the Congress of the United States. Whatever passes the Senate still has to go to a conference with the House. The House's approach on this is very different, and we are going to have to do even more negotiating and give-and-take. I appeal to my colleagues, make a principles vote and vote in a way that says to the country and to your constituents two things: One, you recognize we are in a cyber war now and we are inadequately defended. Second, by voting for cloture,

which means we will take up the bill, you are saying we are willing to work together across party lines to try to get something done.

In my opinion, it is the only way we are going to get to this bill. If cloture is not granted, as disappointed and angry as I am going to be, I will not be petulant. I will be open today, tomorrow, and as long as we have an opportunity in this session, to work with my colleagues to try to reach an agreement that will help us improve our cyber defenses.

Sometimes in moments of disappointment, I go back to the great Winston Churchill. I will just read a few comments from him. These were all in the 1930s when he was in the House of Commons and was concerned that England and the world faced a threat which they were not acknowledging, the rise of Nazi Germany. First, he said this—and I hate to say it, but it relates to where we are today. He said this about those who refused to act decisively to counter the clear and growing threat of a resurgent and rearmed Nazi Germany during the 1930s: ''They go on in strange paradox, decided only to be undecided, resolved to be irresolute, adamant for drift, solid for fluidity.''

I am afraid that is the message we are going to send to the country and to our enemies if we don't get together and pass a cyber security bill in this session. Churchill said he was staggered, after his long parliamentary experience with the debates he had gone through on this question during the 1930s, by two things: ''The first has been the dangers that have so swiftly come upon us in a few years, and have been transforming our position and the whole outlook of the world.''

That is where we are with regard to cyber war, although most people don't understand that. We do. He said:

> Secondly, I have been staggered by the failure of the House of Commons to react effectively against those dangers. That, I am bound to say, I never expected. I say that unless the House [finds its resolve] we will have committed an act of abdication of duty.

I end with those words. I think it is that serious. If we don't find a way either by voting for cloture today to get on the bill so we can negotiate or continuing to negotiate if cloture fails, it will be quite simply a colossal abdication of duty to the people of the United States and their security.

Mr. COATS. Will my friend yield me some time?

Mr. LIEBERMAN. Yes; I yield to my friend from Indiana.

Mr. COATS. Mr. President, first of all, I commend all the Republicans and Democrats who have worked so hard together—nearly one-fifth of us in this Congress—hour after hour, meeting after meeting, and flexibility has been provided to both sides by Senator LIEBERMAN, Senator COLLINS and their bill and Senators CHAMBLISS, MCCAIN, HUTCHISON, and others in terms of trying to reach a consensus. Those who listened to the Senator from Maryland yesterday know we are given the unclassified version of the nature of this threat. Add to that the classified version, and it is truly a threat that needs to be addressed.

It is despicable that the majority leader of the Senate, when we were so close to putting together something to bring joint support of what everybody knows we need to do and want to do—so close with agreements from Democrats and Republicans, ranking members and chairmen of the relevant committees, and presenting a package which would grant limited time and limited germane amendments—to deny us that opportunity.

Yet here we are faced with a dilemma of an imminent threat facing the people of the United States of America and a vote whether to continue the process, continue to work with something that potentially could kill this for the rest of the session and maybe even next year or something that grants to the White House an abuse of executive power to mandate things through executive order, which we have seen on a number of other occasions. Maybe that is the motive, maybe it is not; I don't know.

Nevertheless, we are faced with a critical choice in terms of an imminent threat to the security of the United States and the American people. I hope my colleagues will take that into consideration when we decide what to do. I thank people on both sides for their tremendous efforts, and we should not point fingers of blame at each other.

That is a real effort to join and address this very serious threat to the United States.

I thank my friend and yield back to him.

The PRESIDING OFFICER. The Senator from Connecticut.

CLOTURE MOTION

The PRESIDING OFFICER (Mr. BROWN of Ohio). All time has expired. The clerk will report the motion to invoke cloture.

The 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 is 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 legislative clerk called the roll.

Mr. KYL. The following Senators are necessarily absent: the Senator from Illinois (Mr. KIRK) and the Senator from Florida (Mr. RUBIO).

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

The yeas and nays resulted—yeas 52, nays 46, as follows:

[Rollcall Vote No. 187 Leg.]

YEAS—52

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

NAYS—46

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

NOT VOTING—2

Kirk	Rubio

The PRESIDING OFFICER. On this vote the yeas are 52, the nays are 46. Three-fifths of the Senators duly chosen and sworn not having voted in the affirmative, the motion is rejected.

The majority leader is recognized. The Senate will be in order.

Mr. REID. I enter a motion to reconsider the vote by which cloture was not invoked.

The PRESIDING OFFICER. The motion is entered.

The majority leader is recognized.

Mr. REID. Mr. President, we expect one more vote today. I have not had a chance to discuss it in detail with Senator MCCONNELL yet, but we hope to have a vote on a judge. We hope to have it at 2 o'clock today, so people should make their schedules accordingly.

AFRICAN GROWTH AND OPPORTUNITY ACT—Continued

The PRESIDING OFFICER. Under the previous order, the question is on agreeing to amendment No. 2771 offered by the Senator from Oklahoma.