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 clothe 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 move 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 an enormous 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 clothe on would be a step forward. 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, Afghan-

The Chamber of Commerce has now interjected themselves in the security of this Nation. They think they know more than 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 because anybody is truly op-

So this is a very simple, straight-

This place is so manipulated, I could not 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 impact is, the Senate says, go 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 rec-

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. We do not charge it to our kids because the his-

So this is a very simple, straight-
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 waiting for the southeast 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 follow; 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. 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. 271.

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 271.

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 PROVISION.—Section 121(e)(1) of the African Growth and Opportunity Act (19 U.S.C. 3702(e)(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. 3701(2)) is amended by inserting after “Republic of South Africa” (South Sudan).”:

“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 DULICATING EXPENSES OF THE AGENCY, AND OVERLAPPING 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; and

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—

(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 legisla-
tive changes required to further eliminate, consolidate, or streamline Federal programs and Federal agencies with duplicative or overlapping missions.

The ACTING PRESIDENT pro tempore. Who yields time?

Mr. COONS. Mr. President, I rise today to speak both in favor of the passage of this 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 important legislation. 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 his proposal for 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 will lose the bipartisan support. 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.

As 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 get out of session later today, and every day we delay in the real United States, in APOD provisions 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 timing of this choice is one of the most promising continent for countries willing to invest in long-term partnerships in the United States. In Africa—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 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 yes on AGOA 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 that 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 business-friendly, and 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 of $81 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 the United States to compete 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 of $81 billion last year, growing at a pace that exceeds our exports to the rest of the world.

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 that 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 business-friendly, and 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 of $81 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 the United States to compete 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 of $81 billion last year, growing at a pace that exceeds our exports to the rest of the world.

Mr. ISAKSON. Mr. President, I rise for just a moment to do two things. First of all, I spent 33 years selling homes as a real estate broker, 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 do not wish to say second, or to say 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 Senator Coons 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. 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 century in the past, China is the 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 Georgia 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 constituent Senator Coons 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. We also know that if we actually charge 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 and get to 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 Senator Coburn had voted 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 country’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 country is 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. It is not about doing 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 the vote between self-fulfilling in terms of driving 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 Oklahoma. 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 are 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 proposal 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 and providing, of moving forward with relevant Burma sanctions, and of moving forward with an important technical fix to CAPTA.

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 include close to $200 million in the cybersecurity 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 cybersecurity 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.

The 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 implosions do we need from our Nation’s top homeland and military officials to act on what many believe to be the greatest threat to our national security? 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 could 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 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 is urgent and assessed 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 some 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 opponents. Is that correct? I would ask unanimous consent that the Republican 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.

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 only have we not been discussing the 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 compromise in the spirit that we all like 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, BURK, and McCaskill. It is 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 negotiate seriously. 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 or 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.

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 Senators 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. 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. Let me read this letter for this vote. Cloture will not be invoked. All it will do is embed people in their previously held positions. What we should be
The basic philosophical difference we have been working very hard to prevent those attacks by constantly updating, and investing heavily in our security systems, work tirelessly, day and night, to block cyber-attacks, including working with the federal government and the private sector.

Our sector recognizes the very real and ongoing threat cyber-attacks pose. We recognize that there is a vast gap in the nation’s critical infrastructure from cyber-attacks, this legislation threatens to undermine the critical security protections already in place for our customers and institutions, and misses an opportunity to substantially improve cyber threat information-sharing and collaboration between the federal government and the private sector.

Our industry as we continue to improve the effectiveness of our cybersecurity.

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 companies to share that same information, unfortunately does not allow manufacturers reducing companies’ liability, the legislation.

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.

The Senate to pass legislation that accomplishes this.

The Senate to pass legislation that accomplishes this.

The Senate to pass legislation that accomplishes this.
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 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 are responsible for 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 uncertainty of the United States is directly related to our cybersecurity. The NAM and all manufacturers remain intensely committed to securing our nation's cybersecurity framework 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 cybersecurity. But politically, using efforts to protect financial systems and power grids from hackers, terrorists or rogue states.

The Senate is due to take up cybersecurity 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 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. SEN. KEITH AXELANDER, commander of the U.S. Cyber Command, said that he rates US. 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 a fast-changing fast-changing fast-changing 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 markup up by any 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 this bill 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. SNOE. Mr. President, I rise today to express my strong support for finding a path to legislation that will establish attribution for these incidents.

HUTCHISON, who has worked tirelessly on cybersecurity defense to protect our nation’s economic security, made by the majority leader at

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; 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 rests at risk, and we have to 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 polemics 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 jurisdictional issues and how the matter may be 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 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 inadequate 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 move to a vote 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 I believe it is essential to begin by elucidating the nature of the indispensible threat we now face.

In 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 infrastructures and the cyber space we inhabit. After reviewing the report, my colleagues and I concluded that the United States is not prepared to prevent, detect, and respond to malicious cyber intrusions.

As far as examples we can discuss in an open forum, for instance, the 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.

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 Government is certain that 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 company operations that could benefit China’s ability to exploit its large natural gas and fossil fuel fields.

As the report notes, such activity on behalf of our economic rivals underlines 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 $500 billion or more in terms of loss of data and intellectual property.

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, as well 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 capitol 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 defense measures.”

At 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 today 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 digital and private assets that are the foundation of 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 for 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 cyberspace.

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 2009, 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.

The Senate Cybersecurity 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 of our legislation, which 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 me 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—not 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, 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 critical infrastructure 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 for over-regulation by the Federal Government.

For example, I have heard concerns from the private sector that subsection 109(g) of the revised bill may cause companies 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 made 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 and 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 their critical infrastructure networks whose disruption would in-catastrophic economic damage, or severely degrade national security.

The Rockefeller-Snowe Cybersecurity Act is a necessary and important step in protecting our national infrastructure. 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 critical infrastructure 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 for over-regulation by the Federal Government.

For example, I have heard concerns from the private sector that subsection 109(g) of the revised bill may cause companies 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 made 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 and 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.
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 to have the appropriate capabilities.”

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. 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 the Senate passed last week, 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 America’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 further require agencies 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 becomes patchy at best. 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 agreements. This officer would also be responsible for assessing the privacy impact of the new information-sharing provisions in the cyber security bill. Normally, 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 privacy violation, 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 national security is one of the most challenging 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 priorities that must be a part of our national strategy for cybersecurity.

A legislative response to the growing threat of cybercrime must be a part of our debate about cyber security. Protecting American companies 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 Video Privacy Protection Act, VPPA, and the Electronic Communications Privacy Act, ECPA. The amendment also updates the VPPA keep pace with how most companies and businesses that maintain databases of personal information are now managing the threats to American’s privacy and security in cyberspace.

The amendment also expands the provisions of the Computer Fraud and Abuse Act to address the growing threat of cybercrime. It updates the key provisions of the Electronic Communications Privacy Act, ECPA, that I authored several years ago—the key privacy law that is critical to business, government investigators and ordinary citizens.

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, 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 #3590 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, and for the hundreds of millions of Americans who use mobile phones and the Internet.
for citizens who have won 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; Association of American Libraries; Association for Computing Machinery; Citizen's Corps of America; Consumer Electronics Association; CAUCE North America; Center for Democracy & Technology; Center for Financial Services Innovation; Competitive Enterprise Institute; Computer and Communications Industry Association; Constitution Project; Democracy 21; Defend Democracy Software Association; Game Developers Association; Howard Institute; International Laboratory for Research on Non-Violence; Linux Foundation; Mozilla; NetChoice; Open Web Applications Alliance; Project Afire; Public Knowledge; Public Library Association; Rally For Inclusion; Software Freedom Law Center; TechAmerica; TRUSTe; U.S. Policy Council of the Association for Computing Machinery.

U.S. Senate, Washington, DC.

[Signature]

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 who work 24/7 to inject malware, 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 strong support for recent changes 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 create new offenses such as violations of terms of service, with an Internet service provider, Internet website, or non-government employer. If such violations constitute the sole basis for determining that access to a protected computer was unauthorized, the amendment passed with bipartisan support, including that of Chairman Leahy himself.

As we noted in our previous letter, our concern is that the existing language of the CFAA is so broad and unenforced that any 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" in the physical world. If, for example, an employee photocopies an employer's document to give to a friend without that employer's permission (though there may be, for example, a contractual violation), However, if an employee emails that document, there may be a CPAA 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 CPAA 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 encourage further changes to the language in the bill to ensure that government employees are given the same protections from criminal prosecution as their counterparts in the private sector. 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 Liberty Project; Beryl W. Neustar; Personal; Salesforce; Sonic.net; SpiderOak; Symantec; TechFreedom, TechAmerica; TRUSTe; U.S. Policy Council of the Association for Computing Machinery.

TECHAMERICA, Washington, DC, July 30 2012.

Re U.S. Senate Proposed Cybersecurity Legislation

Hon. HARRY REID, Majority Leader, U.S. Senate, Washington, DC.

Hon. MICHAEL J. DE MINT, Majority Leader, U.S. Senate, Washington, DC.

DEAR MAJORITY LEADER REID AND MINORITY LEADER MCCONNELL: On behalf of our companies, 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 supports the House and the Administration's goals of improving our cybersecurity posture. Specifically, TechAmerica endorses the following provisions of S. 3414 to address our country's critical cybersecurity priorities:

Title V—International Cooperation: We support Title V of S. 3414 which would create a national cybersecurity R&D plan to help develop game-changing technologies that will neutralize cyber threats. We urge Congress to work with the Administration to enact these provisions 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 Acquisition Risk Management: 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 systems.

Title VI—International Cooperation: Cybercrimes are borderless, and we must work with our international partners to combat this threat. Title VI will help protect and enhance critical infrastructure 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 Feinstein.

TechAmerica is confident that these core components alone would immediately and substantially improve America’s cybersecurity posture, and cannot afford the long 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 need further refinement in order for it to receive our overall support as a final cybersecurity proposal. These provisions include:

Title II—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 appreciate this positive approach, TechAmerica recommends further refining the following provisions of Title I.

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

Incentivizing 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 understand the sponsors’ efforts 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 included as part of that proposal. 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 and strengthened private 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 legislation to a limited list of “cyber threat indicators.” Previously proposed language had allowed companies to monitor for cybersecurity threats, which could include actions such as tailoring to steal, access or exfiltration, manipulation, or impairment to the network or data. It isn’t clear that industry’s standard monitoring practices fall within the parameters of the more specific list as some threats are not categorized until after they have been identified. 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 will lead to significant limitation to put our activities 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 expanded.

Voluntary Disclosure of Cybersecurity Threat Indicators Among Private Entities—Business to business information sharing is an important piece to curbing 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 further inhibit 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 private entities would receive when sharing information with the newly created government exchange.

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 grouped 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 reduce 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 today.

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 on which the congress can pass when it comes to ensuring our national security, the National Defense Authorization Act, which includes cyber security elements, has not been submitted. The Senate budget 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 mark-up or normal committee process—should not have taken precedence over a bill which was vetoed 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 time and 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 that we should 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 decisions reliant on 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 information sharing provisions, the critical infrastructure language grants too much authority to the government, failing to consider the innovative potential local and state 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 cybersecurity legislation in 2009, committees have held more than 20 hearings across at least seven different committees specifically on cybersecurity and related legislation, and addressed critical questions relating to cybersecurity in dozens of additional hearings. They held numerous briefings for Senators and staff on cybersecurity, including a simulated cyberattack exercise for all Senators conducted by senior administration officials. They have organized several other forums for Senators to examine cybersecurity issues, including cross-committee working groups designed to develop comprehensive legislation, as well as the Intelligence Committee’s 2010 Cyber Security Task forces. They have held nearly 20 separate cybersecurity bills and numerous cybersecurity-related amendments. And they have held markups of cybersecurity 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 authorities necessary to boost our Nation’s cybersecurity.

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 clear understanding 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 making 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 the 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 actions alone are sufficiently 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, as they increasingly attempt to hold our Nation’s core critical infrastructure at risk.”

Similarly, Secretary of Defense Leon Panetta stated, “We talk about nuclear war and 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 to order in their testimony before 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 cyber security 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 square with the reality of stepping out of step with the patriotism of the owners and employees of 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 our Nation faces 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 help us get this bill through 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 temore. The Senator from Connecticut is recognized.

Mr. LIEBERMAN. Mr. President, I rise to speak on the vote we will have in about 20 minutes. It is 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 terror 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 with al-Qaeda acknowledging it as 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 want 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—no 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 the final passage and the Senate would work its will.

Unfortunately, we haven’t been able to agree on such a list. There are still non-germane, irrelevant amendments on the list. Our friends in the Republican caucus have said yes to the Chamber of Commerce to the vote in a way that says to the country and our constituents, “We believe you are a cyberspace being attacked. We are going to do what the Chamber of Commerce wants us to do. We don’t believe the Chamber of Commerce is acting in the best interest of America, but we are going to do what the Chamber of Commerce wants us to do. We are going to pass a bill that is a pale imitation of what we should pass and will leave the Nation vulnerable.”

Are we going to act before we get to the cyber 9/11? Are we going to act before we get to the cyber 9/11? Are we going to act before we get to the cyber 9/11? Are we going to act before we get to the cyber 9/11? Are we going to act before we get to the cyber 9/11?

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 can get 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 committee. Whatever the House has done 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 we are going to do what the Chamber of Commerce wants us to do. 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, I disagree. This is not an angry, I am hoping 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 cybersecurity.

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 re-armed Nazi Germany during the 1930s: “They go on in strange paradox, de- cided 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 cybersecurity bill in this session. Churchill said he was staggered by the 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 effec- tively 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 con- tinuing to negotiate if cloture fails, it will be quite simply a colossal abdica- tion 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 LIE- BERMAN, Senator COLLINS and their bill and Senators CHAMBLISS, MCCAIN, HUTCHISON, and others in terms of try- ing to reach a consensus. Those who

listened to the Senator from Maryland yesterday know we are given the un- classified 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 disturbing 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 Demo- crats and Republicans, ranking members of the relevant com- mittees, 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 peo- ple 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 exec- utive 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 con- sideration when we decide what to do.

The legislative clerk will report the motion to invoke cloture.

The legislative clerk read as follows:

CLOTURE MOTION

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

The undersigned Senators, in accord- ance with the provisions of rule XXII of the Standing Rules of the Senate, hereby move to bring to a close on S. 3414, a bill to enhance the security and resiliency of the cyber and communications infra- structure 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
Berenstien
Bennett
Bingaman
Binnenthal
Boxer
Brown (MA)
Brown (OH)
Cantwell
Carson
Carper
Casey
Cochran
Collins
Conrad
Donnelly
Durbin
Feinstein

Mikulski
Reed
Rockefeller
Sanders
Schumer
Shibin
Snowe
Shouse
Udall (CO)
Udall (NM)
Warner
Webb
Whitehouse

NAYS—46

Alexander
Ayotte
Barrasso
Baucus
Baucus
Baucus
Burr
Chambliss
Coburn
Coehorn
Corbey
Coryn
Craps
Cruz
Enzi
Graham

Paul
Portman
Pryor
Reid
Risch
Roberts
Sessions
Shelby
Tester
Thune
Toomey
Vitter
Wicker
Wyden

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 recon- sider 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.