



United States
of America

Congressional Record

PROCEEDINGS AND DEBATES OF THE 112th CONGRESS, SECOND SESSION

Vol. 158

WASHINGTON, THURSDAY, JULY 26, 2012

No. 113

Senate

The Senate met at 9:30 a.m. and was called to order by the Honorable MICHAEL F. BENNET, a Senator from the State of Colorado.

PRAYER

The PRESIDING OFFICER. Today's guest Chaplain, Rev. John Fuller, senior pastor of Prairie Lakes Church in Cedar Falls, IA, will lead the Senate in prayer.

The guest Chaplain offered the following prayer:

Let us pray.

God of all nations and all peoples, we come before You on this day acknowledging You as the sovereign Lord of this Nation and of the whole world.

Father, it is a privilege to pray for these lawmakers, knowing that You hear and respond to the prayers of Your people. I pray for these women and men, whom You have put in this position, that they would be filled with Your wisdom to make wise choices and decisions as they lead this country. I pray that this body will be courageous, that they wouldn't be led by fear or their own personal desires but they would have the courage to lead with conviction that comes from You. Give these Senators strength to lead well through difficult times, that they would be strengthened in their inner being by a power that only comes from You.

And, Father, I pray for a spirit of humility that recognizes that others are more important than we are and that You have plans that are greater than ours; that, Father, we would lead with humble and gracious hearts.

We pray all this in Jesus's Name. Amen.

PLEDGE OF ALLEGIANCE

The Honorable MICHAEL F. BENNET led the Pledge of Allegiance, as follows:

I pledge allegiance to the Flag of the United States of America, and to the Republic for which it stands, one nation under God, indivisible, with liberty and justice for all.

APPOINTMENT OF ACTING PRESIDENT PRO TEMPORE

The PRESIDING OFFICER. The clerk will please read a communication to the Senate from the President pro tempore (Mr. INOUE).

The assistant legislative clerk read the following letter:

U.S. SENATE,
PRESIDENT PRO TEMPORE,
Washington, DC, July 26, 2012.

To the Senate:

Under the provisions of rule I, paragraph 3, of the Standing Rules of the Senate, I hereby appoint the Honorable MICHAEL F. BENNET, a Senator from the State of Colorado, to perform the duties of the Chair.

DANIEL K. INOUE,
President pro tempore.

Mr. BENNET thereupon assumed the chair as Acting President pro tempore.

RECOGNITION OF THE MAJORITY LEADER

The ACTING PRESIDENT pro tempore. The majority leader is recognized.

CYBERSECURITY ACT—MOTION TO PROCEED

Mr. REID. Mr. President, I now move to proceed to Calendar No. 470, S. 3414, which is the Cybersecurity Act.

The ACTING PRESIDENT pro tempore. The clerk will report.

The assistant legislative clerk read as follows:

Motion to proceed to Calendar No. 470, S. 3414, a bill to enhance the security and resiliency of the cyber and communications infrastructure of the United States.

Mr. REID. Mr. President, I would now yield to the senior Senator from the State of Iowa, Mr. GRASSLEY.

The ACTING PRESIDENT pro tempore. The Senator from Iowa.

PASTOR JOHN FULLER

Mr. GRASSLEY. Mr. President, it is my privilege to introduce Pastor John Fuller to my fellow Senators, and I

thank Pastor Fuller for opening the Senate with prayer. It is my privilege to highlight my home pastor and church.

Pastor Fuller and his wife Kay are visiting the Nation's Capital this week.

Since 1998 Pastor Fuller has been the senior pastor at Prairie Lakes Church in Cedar Falls, IA. Pastor Fuller is a native of Iowa. He was born in Onawa and grew up in Sloan. His family moved to Sheridan, WY, when he was in the eighth grade. He graduated from high school in Sheridan. He played both high school and college football. He is to this day obviously a die-hard Broncos fan. You won't know that, but I sure know it. He is a 1986 graduate of the University of Sioux Falls and a 1990 graduate of Denver Seminary with a master's of divinity degree.

He was an associate and preaching pastor at First Baptist Church in Forest City, IA, before coming to Cedar Falls in 1998, to Prairie Lakes Church, and has been senior pastor. I have been worshipping at Prairie Lakes Church for 58 years come this August 29. The church has changed its name and increased its congregation over the years, but its heart has remained the same and very constant.

In 1855 a small group known as the Baptist Society started this church. In 1862 it became the First Baptist Church. The first 45 years that I worshipped at First Baptist Church, at various times the congregation numbered 200 to 300 people. Under Pastor Fuller's leadership, the number of worshipers has grown to about 2,000, with worship centers in Osage, Waterloo, and soon in Grennell, IA, besides the main campus in Cedar Falls, IA. In 2005 a new building was constructed, and the name of the congregation then became Prairie Lakes Church.

The worship service is very informal. That has changed in the 58 years I have attended there, but the service has always been Christ-centered, and that has not changed. Prairie Lakes Church

● This "bullet" symbol identifies statements or insertions which are not spoken by a Member of the Senate on the floor.



Printed on recycled paper.

S5419

is multigenerational, with an extraordinary vision for the future. Worship services are heartfelt, creative, practical, Bible-based, and here to serve Christ and here to serve all—those who just stepped over the faith line as well as those who have been longtime followers of Jesus Christ.

Prairie Lakes Church is affiliated with the Baptist General Conference. Prairie Lakes Church is all about loving God, loving people, and influencing the world. Everyone is invited to worship with us—including anybody here in Washington, DC—through streaming online at prairielakeschurch.org.

In closing, I would remind all, according to the Scriptures, in Corinthians, we are all called to be ambassadors of Christ, and that is how I see Pastor Fuller.

I am also grateful to Pastor Fuller for his leadership and faithfulness to this congregation. After 58 years, in my looking back, I know God's word has been preached faithfully at this congregation. Pastor Fuller has contributed significantly during his tenure and continues to do so.

This is what Pastor Fuller had to say about our church:

There are a lot of good churches around the valley. We're lucky to have that. I think people get attracted here because we just stick with the Bible. We're authentic. We're invitational, and we try to keep things simple.

These attributes have attracted many, and I believe they will continue to attract many more and the church will continue to grow.

Lastly, I pray that God will continue to shine His light through Pastor Fuller, his family, and the Prairie Lakes congregation. It is my privilege once again to introduce Pastor Fuller to this Senate.

I yield the floor.

The ACTING PRESIDENT pro tempore. The majority leader.

Mr. REID. Mr. President, I appreciate my friend's remarks about his pastor. They were very well thought out, and I appreciate them very much.

SCHEDULE

Mr. REID. Mr. President, the first hour here today will be equally divided and controlled between the two leaders or their designees. The majority will control the first half and the Republicans the final half.

I filed cloture last night on a motion to proceed to the cybersecurity bill. I hope we can reach an agreement to have that cloture vote sometime today. If not, we will have it tomorrow.

When a major storm ripped through the Mid-Atlantic region last month, it left millions of people without power—I repeat, millions of people. I was at my home here in Washington, which is different from my home in Searchlight, NV. In Searchlight, the wind blows a lot, so you can hear the wind. It is kind of pleasant for me. But the wind we heard at our home in Washington was not pleasant. At 9:30 or 10:00 at night, it was loud and it was abusive and it was, quite frankly, a little scary.

Our power was not affected, but that wasn't the case for millions of other people. Residents of Maryland, Virginia, West Virginia, Ohio, and the District of Columbia soon realized how quickly a major power outage can alter life as we know it. I talked to Senator MANCHIN of West Virginia, and a week later power was still out in large parts of West Virginia. He said it was the worst storm they have ever known in West Virginia.

This power outage altered life as people knew it here in the entire eastern part of the United States. The blackout was devastating to many families and many businesses. But it was also minor compared to the devastation that malicious cyber terrorists could wreak with a single keystroke. I repeat, as damaging and frightening as this storm was, we could have a malicious cyber attack by terrorists that would be far more devastating than this violent storm. Cyber attackers could all too easily shut down the electric grid for the entire east coast, the west coast, and the middle part of our country. Any one attack could leave dozens of major cities and tens of millions of Americans without power. We know, because we were shown in a room here in the Capitol, how an attack could take place and what damage it would do, so we know this is not just make-believe.

Without ATMs or debit card readers, commerce would immediately grind to a halt. My daughter, who lives here in the DC area, lost power when the storm hit. They waited for a number of hours, and then they took all the food out of their freezer, they gave away what they could, and they threw the rest away. And that was the way it was all over. Their power was out for about a week, and it made it very difficult. They are fortunate enough to have a basement, and the heat wasn't oppressive down there.

Without refrigeration, food would rot on the shelves, the freezers would have to be emptied, and people could actually go hungry. Without gas pumps, transportation arteries would clog with abandoned vehicles. Without cell phones or computers, whole regions of the country would be cut off from communication and families would be unable to reach each other. Without air-conditioning and without lifesaving technology and the service of hospitals and nursing homes, the elderly and sick would become much sicker and die. Most major hospitals have backup power, but it is only for a limited amount of time. It depends on how much fuel they can store, and that is very limited.

The devastation is really unimaginable, but we have heard these ominous scenarios before. What many Americans haven't considered is that the same power grids that supply cities and towns, stores and gas stations, cell towers and heart monitors also power every military base in our country. About 99 percent of electricity used to

power military installations comes from outside the bases. Nellis Air Force Base, one of the largest in the world of its type, has some solar energy there that they have developed, but over 90 percent of their power, in spite of that, comes from outside the base, and more than 85 percent of that power is provided by the same electric utilities that power homes and businesses and schools in the civilian world. So a cyber attack that took out a civilian power grid would also soon cripple our Nation's military—very soon.

Although bases would be prepared to weather a short power outage with backup diesel generators, within hours, not days, fuel supplies would run out. Command and control centers would go dark. Radar systems that detect air threats to our country would shut down. Communication between commanders and their troops would go silent. And many weapons systems would be left without either fuel or electric power.

Much of what we do militarily is now done by computers and done very remotely. It is no secret that the drones that operate for our country all over the world are not operated from Pakistan, Afghanistan, or Somalia, they are operated from a base 35 miles outside Las Vegas. That is all done with electricity. So in a few short hours or days, the mightiest military in the world would be left scrambling to maintain base functions.

That is why our top national security officials—including the Chairman of the Joint Chiefs, the Director of the National Security Agency, the Secretary of Defense, and the CIA Director—have said that the kind of malicious cyber attack I have just described is among the most urgent threats to our country. In fact, they have said that unless we do something and do it soon, it is not a question of if, it is only a question of when.

There have already been cyber attacks on our nuclear infrastructure, our Defense Department's most advanced weapons, the NASDAQ stock exchange, and most major corporations. These are just a few of the things that have already been attacked by cyber.

Senator MCCONNELL and I recently received a letter from a bipartisan group of former national security officials, including six former Bush and Obama administration officials, that presented the danger in stark terms:

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

That is what they said, not me. The group said the threat of cyber attack "represents the most serious challenge to our national security since the onset of the nuclear age sixty years ago."

The bill before this body, proposed by a coalition of Democrats and Republicans—including Chairman LIEBERMAN

and ranking member COLLINS—is an excellent piece of legislation endorsed by many members of the national security community.

In my view, it is not strong enough, but it is a tremendous step forward, and I admire the work they have done. I know some of my colleagues have suggestions on how to improve this legislation. I have a few of my own. There is plenty of room for good ideas. Some of them are already on the table. It is my intention for Senators to have an opportunity to have a robust debate on these proposals. Let's stick with what this bill is all about and let's have as many amendments as people feel is appropriate.

The national security experts agree we can't afford to waste more time. The question is not whether we should act but whether we will act in time.

As I mentioned at the start, we are scheduled to have this vote an hour after we come in tomorrow. I am working with Senator MCCONNELL now to try to arrange a time, perhaps even today. My goal is to get on the bill. I hope we can get on the bill. It would be terrible for our country if we are not on the bill. I would like to get on the bill and have Senators LIEBERMAN, COLLINS, ROCKEFELLER, FEINSTEIN, and the other committees that are involved come up with a list of amendments as we have done so well on a number of the bills we have worked through. When we come back next week, let's start doing some legislating and have some robust debate, get some of these amendments disposed of, and pass this bill on to the House.

The House has done their bill. We can go to conference and get something done. It would be very important for our country.

RECOGNITION OF THE MINORITY LEADER

The ACTING PRESIDENT pro tempore. The Republican leader is recognized.

THE ECONOMY

Mr. MCCONNELL. Mr. President, yesterday our Democratic friends took a vote that says a lot about the way they view the world. After nearly 4 years of spending and debt, millions of Americans are still struggling amidst the slowest recovery in modern times, and the economy is flat on its back. Our friends on the other side think a great way to go forward is to raise taxes. Under the guise of pretending to care about the deficit, Democrats are pushing an ideological goal of a symbolic tax increase that would not even fund the government for 1 week. The vote we had yesterday—with all but two of the Democrats on board—allegedly doing something about the deficit wouldn't fund government for 1 week.

They are not even pretending to care about the economy. They have sort of given up on the argument that this is about the economy. We know that because 2 years ago the Democrats agreed the higher taxes they are now fighting for would hurt the economy.

Let's look at the economy then and the economy now. At a time when eco-

nomics growth was 3½ percent, back in December of 2010, 40 Democrats voted to keep rates where they were on the grounds that it was the best thing to do for jobs. In December 2010, 40 Democrats voted to keep the tax rates where they were because it was the best thing for jobs. Yet now when the growth rate is 2 percent—it was 3½ percent then, it is 2 percent now—and 13 million Americans are still out of work, they are voting to slam nearly 1 million businesses with a tax increase. Maybe they are expecting the GDP numbers tomorrow to be 3½ percent. We will see.

That is one of two things, either our Democratic friends don't even care about the economy and jobs anymore and are just embracing Thelma-and-Louise economics—let's take everybody off the cliff and hope people support them for some other reason—or their economic world view is so far outside the mainstream of everyone else who has looked at the situation that they think 2 percent growth and 13 million Americans unemployed is good enough. Maybe they think that is as good as we can do. That is where this ideological crusade of theirs is taking them, right in that direction. I just hope for the sake of a struggling American economy that some of them soon see how misguided an approach this is.

Let me repeat, 2 years ago in December of 2010, when the economy was growing at a rate of 3½ percent, 40 of our Democratic colleagues, the President, the Vice President, me, and the Speaker agreed to extend the current tax rates for 2 years because it would be good for jobs.

Just yesterday, with two exceptions, every Democrat voted to raise taxes on 1 million businesses when the growth rate—the GDP increased rate—is 2 percent and 13 million Americans are looking for work. That is not a prescription for the economy; that is an ideological crusade. That is not about America's jobs; that is about the election 4 months from now.

I yield the floor.

RESERVATION OF LEADER TIME

The PRESIDING OFFICER (Mr. MANCHIN). Under the previous order, the leadership time is reserved.

ORDER OF BUSINESS

Under the previous order, the following hour will be equally divided and controlled between the two leaders or their designees, with the majority controlling the first half and the Republicans controlling the final half.

The Senator from Colorado.

PRODUCTION TAX CREDIT

Mr. UDALL of Colorado. Mr. President, I rise to speak on the floor of the Senate again this morning to urge my colleagues to vote to extend the production tax credit for wind energy. It is also known as the production tax credit. I know the Presiding Officer's home State of West Virginia has a robust wind energy sector as well. I look forward to coming to the floor and talking about the Presiding Officer's State in the future.

The reason I am talking about the production tax credit is it is set to expire at the end of this year, and it will cost citizens in my State and the rest of the Nation their jobs. We cannot let this happen. Tens of thousands of vital jobs are dependent on the wind industry all across our great country.

As I have mentioned, I come to the Senate floor on a daily basis and I highlight a State and talk about what the production tax credit has done to encourage economic growth in that State. Today, I wish to talk about the great State of Illinois, the land of Lincoln, where the wind industry is thriving. Illinois is an impressive example of how wind resources can be harnessed and put to good use creating jobs and supporting local communities.

Overall, Illinois has the fourth largest installed wind capacity in the United States, with over 600,000 homes powered by the wind. If fully utilized, the wind energy resource in Illinois could provide 525 percent of the State's current electricity needs. That is truly a staggering amount of electricity for the fifth largest State in the Nation.

In 2011, Illinois was second only to California in the number of new wind energy projects completed, and they installed more wind turbines there than any other State in the country. Clearly, Illinois recognizes the economic potential wind energy holds for the future, as many other States have.

Just last week in Illinois, Invenergy announced it completed construction of the Bishop Hill wind energy facility in Henry County. That is up in the northwestern part of Illinois, near Davenport, IA. The project covers 22,000 acres of farmland and includes over 100 wind turbines and can power 60,000 homes. The Bishop Hill project is clearly a huge investment in Illinois and our Nation's clean energy future. But the economic power of wind energy has been equally impressive. The wind energy there supports 7,000 jobs, it contributes close to \$19 million every year in property taxes to local communities, and Illinois led our Nation in 2011 with over 400 new wind turbines installed.

Just this month, Illinois State University released a report that estimates that the 23 largest wind farms in Illinois will contribute roughly \$5.8 billion to the local economies over the lifetime of these projects. The construction of these wind farms generated over 19,000 jobs that cut paychecks totaling over \$1 billion for workers. These are good-paying, high-skill jobs that we are proud to have in our country and that American workers are proud to have and it is one part of the overall wind energy story.

For example, the Odell Grade School, in Odell, IL, has a much needed project underway that will expand the school and make it more energy efficient. While this project is expensive, it will be paid for, in part, by payments from local wind farms. Wind energy is supporting a better education for Odell's youth without increasing taxes to the local residents.

This is not unique to Illinois. It is happening all across our country. I have no doubt the people of Odell would agree with me that extending the PTC is a commonsense proposal. However, without Congress extending the production tax credit, our country and the wind industry literally face impending disaster. In fact, many wind energy manufacturers and producers have already been preparing for the end of the PTC by backing off their investments in many of these communities such as Odell and by announcing future layoffs of thousands of workers. It is just flatout unacceptable that we in the Congress would let this happen.

I think everyone understands where I am heading. This is a serious issue that needs attention now—not next month, not in the fall, not in the lameduck session but now. The wind industry will not wait for us to extend the PTC at some date in the future. They have already begun to scale back their operations and move overseas. Further inaction is unacceptable. China is stepping into the breach and literally taking our jobs overseas. Other countries are prepared to do the same. For us in Congress to miss this opportunity to not only preserve jobs but put in place policy that would create thousands of good-paying jobs because of election-year gridlock is flatout unacceptable. If we don't act, our people in our States will suffer.

I come to the floor every day to implore my colleagues to extend the wind production tax credit as soon as possible. The PTC equals jobs. We ought to pass it as soon as possible. I will be back next week to continue discussing the wind Production Tax Credit and urge us to be bold, take up this issue and extend the wind production tax credit. It is about American jobs. It is about maintaining our leading position in the world when it comes to clean energy development.

I yield the floor and note the absence of a quorum.

Mrs. MURRAY. If the Senator could abstain from the quorum, please.

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

The Senator from Washington.

VIOLENCE AGAINST WOMEN ACT

Mrs. MURRAY. Mr. President, I come to the Senate floor today in order to continue the efforts started right here earlier this week, efforts by the women of the Senate and the men who support the Violence Against Women Act to bring a simple, straightforward message to our friends in the House of Representatives: Stop the games and pass the inclusive, bipartisan Senate VAWA bill without delay.

The Violence Against Women Act is a bill that has successfully helped provide lifesaving assistance to hundreds of thousands of women and families. It is a bill that passed the Senate 3 months ago today by a vote of 68 to 31. It is a bill that has consistently included bipartisan provisions to address those who are not being protected by it

each and every time it has been reauthorized. But here we are, back on the Senate floor, urging support for a bill that should not be controversial.

Just as we did on Tuesday, just as we are doing today, and just as we are going to continue to do in the coming weeks, we will be making sure this message resonates loudly and clearly both in Washington, DC, and back in our home States because we are not going to back down—not while there are thousands of women across our country who are excluded from the current law. In fact, for Native and immigrant women and LGBT individuals, every moment our inclusive legislation to reauthorize the Violence Against Women Act is delayed is another moment they are left without the resources and protection they deserve in this country.

The numbers are staggering: 1 in 3 Native American women will be raped in their lifetimes—1 in 3. And 2 in 5 of them are victims of domestic violence, and they are killed at 10 times the rate of the national average. These shocking statistics are not isolated to one group of women; 25 to 35 percent of women in the LGBT community experience domestic violence in their relationships, and 3 in 4 abused immigrant women never enter the process to obtain legal status, even though they were eligible, because their abuser husbands never filed their paperwork.

This should make it perfectly clear to our colleagues in the other Chamber that their current inaction has a real impact on the lives of women across America affected by violence, women such as Deborah Parker. Deborah is the vice chairman of the Tulalip Tribe in my home State of Washington.

Deborah was repeatedly abused starting at a very young age by a nontribal man who lived on a reservation. Not until after the abuse stopped—some time around when she was in the fourth grade—did Deborah realize she was not the only child suffering at the hands of that same assailant. At least a dozen other young girls had fallen victim to that man—a man who was never arrested for his crimes, never brought to justice, and still walks free today, all because he committed these heinous acts on the reservation. As someone who is not a member of a tribe, it is an unfortunate reality that he is unlikely to ever be held liable for his crimes.

Reauthorizing an inclusive VAWA is a matter of fairness. Deborah's experience and the experience of other victims of that man do not represent an isolated incident. For the narrow set of domestic violence crimes laid out in VAWA, tribal governments should be able to hold accountable defendants who have a strong tie to the tribal community.

I was very glad to see Republican Congresswoman JUDY BIGGERT and several of her Republican colleagues echo those sentiments last week. They sent a letter to Speaker BOEHNER and Leader CANTOR. These Republican Members

explicitly called on their party leadership to end this gridlock and accept the "Senate-endorsed provisions that would protect all victims of domestic violence, including college students, LGBT individuals, Native Americans and immigrants."

So today I am here to urge Speaker BOEHNER to listen to the members of his own caucus and join us in taking a major step to uphold our government's promise to protect its people, people such as Maribel and Maria, two more constituents who come from my home State of Washington.

As a transgender woman, Maribel has been subject to random acts of violence by family and boyfriends and strangers. She has been mugged and attacked on the street. She has suffered broken bones and cuts and bruises. She has been raped, and she was left for dead. What Maribel said to me was deeply concerning. She said:

Not once have the police ever conducted an investigation, much less shown any concern for me. Rather my experience with law enforcement is one of harassment and abuse. I have been ostracized by family and friends . . . in fact it is most of my first memories.

She experiences hate daily from those who think she has no place in our society.

Then there is Maria. Shortly after their wedding, Maria's husband became a different man, she said. His abuse ranged from emotional to physical, and on two separate occasions he held a knife to Maria's throat threatening to kill her. He constantly threatened Maria with deportation back to Jamaica. Eventually, he refused to attend the interview with immigration authorities necessary for her to obtain a green card. Her application was denied for lack of attendance. She was angry and scared, but she found the courage to ask her husband for a divorce. In response, he raped her. Maria moved out of the house though her husband repeatedly tracked her down and assaulted her. To save her own life, Maria fled to Seattle with her two young children.

It does not have to be this way. I was so proud to have been serving in the Senate in 1994 when we first passed the Violence Against Women Act. Since we took that historic step, VAWA has been a great success in coordinating victims' advocates and social service providers, and law enforcement professionals to meet the immediate challenges of combating domestic violence. Along with its bipartisan support, it has received praise from law enforcement officers and prosecutors, judges, victim service providers, faith leaders, health care professionals, advocates, and survivors.

The Violence Against Women Act has broad support for one reason: It works. Where a person lives, their immigration status, who they love should not determine whether perpetrators of domestic violence are brought to justice. These women cannot afford any further delay—not on this bill.

Mr. WYDEN. Mr. President, would the Senator yield for a question.

Mrs. MURRAY. I would be happy to yield for a question.

Mr. WYDEN. I think the Senator from Washington has made an extraordinary presentation in terms of outlining the facts of the abuse women face. Having done a series of forums around my home State—as my colleague knows, in our part of the country in Washington and in Oregon where there are many small communities of 10,000, 15,000 people, it is my experience—and I would be interested in getting the assessment of our colleague since she has been a leader on this—that without the Violence Against Women Act, it is my understanding that women in rural areas who face the kind of brutal treatment my colleague described would literally have nowhere to turn, so that the Violence Against Women Act for women in rural areas in particular is sort of the last line of defense for them.

Mrs. MURRAY. The Senator from Oregon is absolutely correct. If a woman has been beaten and abused and believes she is a victim of violence with nowhere to turn, especially in a rural community where everyone knows everyone and a person doesn't know who to turn to, there is no place to go. The Violence Against Women Act provides the support of law enforcement officers and advocates so a person can get out of a very abusive situation.

Mr. WYDEN. I am going to listen to the rest of my colleague's remarks, and I will have my own. But I just want to thank the Senator from Washington for her leadership. This is such an important issue. It is not about dollars and cents, and it is not about politics. It is about doing what is right for combating violence, and I commend my colleague.

Mrs. MURRAY. I thank my colleague from Oregon. I know he is going to speak in just a few minutes, but I know he has spent a great deal of time traveling around his State and listening to these women and he knows personally from their stories how important it is that we cannot continue to delay this bill over something called a blue slip. It is not about a blue slip. It is about doing what is right.

We have overcome the blue slip issue time and time again for issues such as FAA and Transportation bills and many other pieces of legislation because it is the will of the body to do so. So to tell a woman in Oregon or Washington State that this bill can't happen because of a blue slip is ridiculous. They have been told they can't get help for a lot tougher reasons. Let's not let a blue slip be what comes between them and the support they need.

In fact, I say to my colleague from Oregon and all of my colleagues that on Tuesday the New York Times ran an editorial that gets to the heart of it. They said:

House Republicans have to decide which is more important: Protecting victims of do-

mestic violence or advancing the harsh antigay and anti-immigrant sentiments of some on their party's far right. At the moment, harshness is winning.

The editorial also echoed our sentiments that it does not have to be this way. It pointed out:

In May, 15 Senate Republicans joined with the chamber's Democratic majority to approve a strong reauthorization bill.

It ends with what we all know it will take to move this legislation forward: leadership from Congressman BOEHNER. So today we are on the Senate floor to make this effort and to call for the same thing: leadership.

It is time for Speaker BOEHNER to look past ideology and partisan politics. It is time for him to hear the stories of women across America who have not had the protection of this bill and to make a major step forward which will assure that a woman, no matter where she lives or who she is, will have the protections this great country can offer.

So I thank my colleague from Oregon for his real passion and understanding on this issue and for taking the time to hear from women and men who have been impacted.

I yield the floor.

The PRESIDING OFFICER. The Senator from Oregon.

Mr. WYDEN. Mr. President, I wish to follow on the very important remarks made by our colleague, Senator MURRAY. As a result of the debate we have had in Washington, DC, I knew there was a significant problem, but until we held these forums across our State—we essentially went into every corner of Oregon—it really didn't come home to me how serious a problem this is.

I wish to highlight for a moment or two this point I got into with Senator MURRAY with respect to rural areas, some of the stories. For example, I was told about a woman in central Oregon who essentially, faced with a very abusive relationship, spent the evening trying to hide out in ditches in the community. She would just run from ditch to ditch. Of course, a person gets pretty banged up and bruised when they do something like that, but she hid out in ditches through the night in order to avoid her abuser.

But then it came to morning time and she wanted to get out. She wanted to get to the Safety Net program, which is a wonderful shelter in her area. But the fact was the only way to get out was to ask for a ride from the one person who had a vehicle in the community, and that was the person who abused her in the first place. So, literally, in a rural community—and I heard this account just recently—she had nowhere to turn. That is why I characterize the Violence Against Women Act as—especially for rural women—the last line of defense between them and the abuser.

In another community—I know my colleague, the Presiding Officer, will identify with this, and I enjoyed going to West Virginia and the like—in a

rural community in the eastern part of our State, it was described to me that there was no transportation out of the community. There was no transportation at all. The woman involved was going to literally have to stay there and face continual abuse. The one vehicle in the community was a fishing shuttle.

I am sure the Senator from West Virginia identifies with that. It is something we have in our rural communities—a vehicle that takes folks fishing.

The owner of the fishing shuttle said: I am going to be the one to take this woman to safety. I don't need to be reimbursed. I don't need to have some kind of government program or something. I am going to do it because it is right.

That is how that woman in a rural community escaped her abuser. She got out. She got free. She was able to shake out of the clutches of the abuser because the fellow who owned the fishing shuttle stuck up for her.

But I think this is Senator MURRAY's point: I do not think we can accept that all across the country we are going to have fishing shuttles available in order to rescue women who are subject to this kind of abuse. I think that is pretty farfetched, and the good hearts of Oregonians came through in that particular situation, but we have to reenact this program.

The fact is, Mr. President and colleagues, this has been the law of the land for more than a decade. There has not been a shred of partisanship in it. It is not about ideology. It is about protecting women from brutality. I had thought, frankly, we had gotten over some of the arguments against this legislation that had been trotted out in the past.

For example, it was often said in the past: Well, maybe these abuse cases are not abuse. Maybe they are just kind of family matters. They are going to get settled when the family kind of calms down. Maybe somebody got upset about something, and then in a day or so everything is going to go back to normal.

That is not the case. This is about repeated instances of violence, repeated instances of violence you cannot slough off as a family difference of opinion. It is a crime. It is brutal violence. That is why we need this legislation, and we need it reauthorized.

I think it is also especially important, given some of the budget cuts we have seen that are particularly hitting small communities like a wrecking ball. For example, in Josephine County—a rural part of our State—they are in the position where, when a subpoena goes out, they essentially do not have the resources to follow it up. In other words, the subpoena is used to, in effect, set in motion the law enforcement process to bring the abuser to justice, and I was told by the key law enforcement officials in Josephine County—in a community forum I held in Medford, OR, for folks from the southwestern

part of the State—that they literally do not have the resources to follow up on how to ensure that abuser is brought to justice.

I would make a couple of additional points. I see colleagues on the floor waiting to speak.

I also want to talk about the costs that are associated with this. You have two kinds of costs. First, you have direct health care costs that stem from the violence you see perpetrated against women, and then also you have costs in terms of lost productivity. At a time when we are getting hit very hard by unemployment—and we know we are in a productivity race with Asia and India and China and other countries—we cannot afford the costs, the health care costs of the violence against women that ends up having women land in hospital emergency rooms and the like, nor can we allow this lost productivity at a time when we are pushing so hard to create more good-paying jobs.

The protection that is offered through the Violence Against Women Act saves my home State of Oregon now millions of dollars through its key provisions. Safety from domestic violence would save Oregon more than \$35 million per year in direct health care costs. Our State loses approximately \$9.3 million per year in lost productivity from paid work as a result of domestic violence. The fact is, the preventive services offered by the Violence Against Women Act saves money, as does the very important work that is done by victim services.

The study of 278 victims in my home town of Portland who received domestic violence and housing assistance found that those services resulted in more than \$610,000 in savings during the first 6 months. So there are savings in terms of assistance, whether it is housing or counseling. Emergency medical care utilization is reduced as a result of emergency services, safety net services being available. Whether it is one measure or another, from a financial standpoint, reauthorizing the violence against women legislation makes sense.

But at the end of the day, while the financial savings are substantial, it seems to me the Violence Against Women Act is about restoring dignity to women who have been abused in our country. No woman in the United States should be subject to the kind of physical abuse I have documented in cases coming from Oregon and that Senator MURRAY has described this morning. They strip our people—women in this country—of their dignity and their confidence and their ability, after they shake free from their abuser, to get on and have the kind of productive life they want for themselves and their family.

Ultimately, this is about dignity. It is about doing what is right. This legislation has been on the books for more than a decade. There is no reason—none whatever—that this legislation is

not passed overwhelmingly on a bipartisan, bicameral basis. I am going to do everything I can here on the floor of the Senate talking with colleagues on both sides of the aisle to make sure this legislation is reauthorized. Because what I saw during these community forums in my home State, from small towns across Oregon, should not happen in my State, it should not happen anywhere, because it is not right, and the Senate can take action to stop it.

With that, I yield the floor.

The PRESIDING OFFICER. The Senator from Arkansas.

PASSING APPROPRIATIONS BILLS

Mr. BOOZMAN. Mr. President, there has been a lot of talk about the dangers of raising taxes during a recession. President Obama famously said in 2009: “You don’t raise taxes in a recession.” Our economy is certainly worse now than it was then. But that did not stop the Senate majority from pushing through a tax increase on our small business owners yesterday.

We need to get our fiscal house in order, and that starts with budgeting in a responsible manner. Washington’s primary problem is not a revenue problem. Washington’s primary problem is a spending problem, and the Senate majority’s actions have exacerbated that problem.

The Senate has failed to pass a budget for the past 3 years. Meanwhile, our country is facing record deficits and an ever-increasing debt. This is the fifth straight year that Washington’s excessive spending has led to a trillion-dollar deficit. It now sits at a jaw-dropping \$15.9 trillion. The Senate majority’s only answer to this crisis is to raise taxes on our job creators during a time while our country has an unemployment rate of over 8 percent.

Along with failing to produce a budget, the Senate majority leader is now backtracking on a pledge to enact every individual appropriations bill this year. Needless to say, I am disappointed. In fact, I think it is safe to say our entire caucus is disappointed.

It was not too long ago that I was down here on the floor praising the majority leader in his efforts and those who would have us go forward and enact our individual appropriations bills. We believed we had a good-faith agreement to move these bills, to make the effort to function the way this body was established to work, to do our job and pass all of the appropriations bills so that the government operates on a budget the way every Arkansan does.

Now the majority is telling us this is not going to happen. Determining how we spend hard-earned taxpayer dollars is a basic responsibility of Congress. We know tough choices have to be made in these appropriations bills, but moving forward is the right direction. The trend of continuing resolutions and giant omnibus appropriations bills has to stop.

Enacting all appropriations bills in regular order would be an important

step to reducing government spending. It would help balance our budget while investing in programs Americans have come to rely on.

Moving forward on these bills would return the Senate to its proper function and provide a framework of spending so the American people can see and understand where their hard-earned money is going. Most importantly, it would help us back away from the fiscal cliff we are hanging on to.

Here is the reality: We borrow around 40 cents of every \$1 we spend. We are running record-breaking deficits every year. The average American family does not have the luxury to live by this sort of budgeting. If you tried to run your household, your business this way, the bank would cut you off. It is time we apply that lesson to Washington.

We are at a crossroads in our country. If we continue down the path we are going, we risk going in the direction of Greece, Ireland, Portugal, and now Spain—each facing economic crises that have pushed them to the brink of default.

If Congress continues the reckless spending, rather than crafting an immediate solution to this crisis, our actions will inevitably lead to an economic collapse. We cannot keep kicking the can down the road, which is exactly what we are doing by passing continuing resolutions and omnibuses after continuing resolutions and omnibuses. It goes on and on.

Each one of us in this Chamber owes it to the American people to work together to help our country today and build a path of success for the future. Our Founding Fathers laid the foundation that allows the Senate to function effectively and efficiently, but it does require us working together.

The American people are tired of the finger pointing that has stalled much of the work they have sent us here to do. That starts with trying to enact all of the appropriations bills through a regular process each year. I sincerely hope the Senate majority leader reconsiders the decision to cancel consideration of the appropriations bills, again, so we can get back to a normal budgeting process, get back to a normal method, an efficient method, a very transparent method, so the American people can see where their taxpayer dollars are going.

With that, I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

The PRESIDING OFFICER (Mr. UDALL of New Mexico). The Senator from Oklahoma is recognized.

Mr. COBURN. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

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

Mr. COBURN. Mr. President, I assume we are out of morning business.

The PRESIDING OFFICER. The Senate is on the motion to proceed to S. 3414.

UNANIMOUS CONSENT REQUEST—S. 3326

Mr. COBURN. Mr. President, I have a unanimous consent request.

I ask unanimous consent that the Senate proceed to the immediate consideration of S. 3326; that the Coburn amendment at the desk be agreed to, the bill, as amended, be read a third time and passed; that when the Senate receives the House companion bill to S. 3326, as determined by the majority and the Republican leaders, the Senate proceed to its immediate consideration; that all after the enacting clause be stricken, and the text of S. 3326, as passed by the Senate, be inserted in lieu thereof; that the bill be read a third time and passed; that a statutory pay-go statement be read, if needed, and passed with no amendments in order prior to passage, the motions to reconsider be considered made and laid upon the table with no intervening action or debate, and any statements related to the bill be printed in the RECORD at the appropriate place, as if read.

The PRESIDING OFFICER. Is there objection?

The Senator from Montana.

Mr. BAUCUS. Mr. President, I reserve the right to object and would like to make a statement.

I am basically opposed to the Senator's request, and let me explain why. The Finance Committee considered this bill last week, and we passed it out of committee by a voice vote without a single amendment being offered. Nobody on the committee offered an amendment. I think we cannot and should not delay the passage now. It passed unanimously, no amendments offered, and now is not the time to delay.

This bill is fully offset. How? By extending customs user fees and corporate timing shift. This is not the first time we have used the corporate timing shift as an offset. I have a list—a very long list—of the many times when this body has used this very same provision and very same offset. In fact, it has been used multiple times since 2005 in trade bills and lots of other bills, so there is much precedent.

I, nonetheless, understand Senator COBURN now has concerns about the offset, and I am willing to work with him to find alternate offsets in future trade measures. We need to move forward on this bill in its entirety as soon as possible. We can't pick and choose to move forward on component parts while leaving others to linger. There are real consequences for delay.

This bill extends provisions of the African Growth and Opportunity Act—otherwise known as AGOA—trade preference program that would otherwise expire in September. Without swift passage of this bill, U.S. retailers do not have the certainty they need to place orders with African apparel manufacturers. Not only are these U.S.

companies struggling to make the best decisions for their companies, but a substantial drop in orders has caused devastating job losses in Africa. The job losses are occurring why? Because of the uncertainty as to whether this provision will be extended. Right now the Senator from Oklahoma suggests we don't proceed.

Another provision of this bill closes a loophole in the Dominican Republic-Central American-United States Free Trade Agreement that will save almost 2,000 yarn-spinning jobs in North Carolina and in South Carolina. And the Burma sanctions provision expires today. These provisions are all necessary parts of the delicate compromise we negotiated in advance with the House and that the Senate Finance Committee approved. Ways and Means Chairman CAMP in the House and Ranking Member LEVIN in the House have made it equally clear they will not pass this bill in the House without the AGOA provisions included. So the House will not pass these provisions if the Senator is successful.

I, therefore, urge my colleagues to pass S. 3326 as it passed from the Finance Committee, quickly and without amendment. For those reasons, I must object.

The PRESIDING OFFICER. Objection is heard.

The Senator from Oklahoma.

Mr. COBURN. Mr. President, short memories are just that. In my opening statement in the Finance Committee on this bill, I made it very clear I opposed the pay-for in this bill. I had two amendments to offer. They were not offered because the chairman had assured me beforehand that he would object and rule them nongermane, even though they were not nongermane. As a matter of fact, we had offered what the Obama administration had already offered in terms of trade duplication—a \$200 million pay-for that the administration supports.

So let's talk about what is really going on here. We are a country that is \$15.8 trillion in debt. We have a process that is not open, really, to the consideration of addressing real pay-fors for a real bill that I agree needs to pass. I have no objection to the underlying policies in any of the three components in this bill, but there is a process we continue to practice which has our country bankrupt. That process is the following: We are going to spend \$200 million over the next 3 years, and then we are going to take 10 years to pay for it.

We have \$350 billion in waste, fraud, and duplication in the Federal Government that we have done nothing about as a Senate. Not one thing have we done to address the issues that are wasting the hard-earned money of the taxpayers of this country. So when we have a small bill and administration concurrence on something that should be eliminated, and yet we would rather not do that but just kick the can down the road, we are failing the American people.

I have a great deal of respect for the chairman of our committee, but it seems to me that my conversations with the Speaker and Mr. CANTOR and Mr. CAMP in the House are much different than his. As a matter of fact, if we were to divide this, they would divide theirs and pass them both back over here, and we could do the same. What I have offered is to separate out these two from the AGOA package. I am for that. I just think we ought to pay for it.

What I have offered, and I offer to do now if the chairman splits it, is to have 30 minutes on the floor to explain why I want to pay for the AGOA, then have a vote, and let it go. But we will not even do that. So not only do we not want to address the problems, we don't even want to have a debate and an opportunity to stand up and say whether we are for cutting wasteful spending, which even the administration is for. That is what is offered.

So now we stand here, with Burma sanctions going to expire. I am going to tell you, I am not moving. I will object to any unanimous consent request that doesn't have a real pay-for for the \$200 million for this bill out of real spending in the next 1 or 2 or 3 years, which is exactly what we offered to put forward in committee and what we have offered to negotiate. I am not going to be a part of kicking the can down the road again. I am not going to be a part of playing gimmicks where we ask corporations to overpay their taxes so we can get around the 1974 Budget Act and pay-go and essentially be dishonest with the American people about what we are doing.

I understand I am not the chairman of the Finance Committee, but I am a member. And I am a Member of this body. Since I had no right in committee to offer an offset because they were ruled—they were going to be ruled nongermane, which they weren't, and now, consequently, we want to ram this through on a timed basis, I am not going to agree to that happening.

So we need to start acting like grownups in terms of our debt and not kick the can down the road 10 years, and that is what we are doing. We are going to use 10 years to pay for something we are going to spend over 3, just like we did on the highway bill, just like we violated pay-go, just like we violated the budget agreement we just agreed to last August. Now we are going to continue to do the same thing.

I have the greatest respect for my chairman. He has been here a long time. He knows a lot about these issues. I agree they need to happen, but they do not need to happen on the backs of taxpayers 10 years from now. We need to pay for what we are doing now.

That is the whole point of this exercise. I want us to be able to have certainty. I want us to have the Burma sanctions continued. I want us to do the right thing. But I want us to do it in the right way, and we are not. So that is where I stand.

I would defer to the chairman for his comments.

The PRESIDING OFFICER. The Senator from Montana.

Mr. BAUCUS. Mr. President, I very much understand the frustration of the Senator from Oklahoma, and I understand his reasons for objecting. In a perfect world, I might be sympathetic with his reasons, but this is not the perfect world. This is a world where we try to do our best to do our work and get legislation passed.

I personally don't have a problem with the Senator's suggestion that we could set 30 minutes aside and vote on his amendment as an alternate way to pay. I think the Senator understands this bill is fully paid for already. It is just the Senator would like it paid for in a different way.

The problem I have in trying to arrange all this and put it together is I can't control other Senators. Other Senators may object to the Senator's provision. They may have their own bills. In fact, I can think of two or three right now who would very much take advantage of a process where the Senator from Oklahoma strips out the bill and offers his own pay-for because they would say: Oh gosh, this is now an opportunity for me to offer mine. That is what they will say to themselves, and then we are really stuck because the Burma provisions expire, as the Senator knows, today. We can't dally. We can't wait. The AGOA provision expires at the end of September.

Now, one could say: Well, wait until the end of September. Unfortunately, a lot of American companies are uncertain whether we are going to extend past the September 30 date, and they are laying off people. Lots of job losses are already occurring as a consequence of the uncertainty. So my job, in putting together these several bills—including PNTR for Russia—in the committee was to talk to Senators and try to find an accommodation where we could get it passed.

I totally agree with the Senator on his main point; namely, how much fraud and waste there is and that it should be addressed and how important it is to get the debt down. As the Senator knows, yesterday, in committee, we talked about ways to address the so-called fiscal cliff, the very beginnings of the Finance Committee's finding solutions to the debt and some kind of grand bargain in the form of tax reform.

The Senator is correct. He did file amendments with alternative offsets, and I did state the amendments would be ruled nongermane. That is true. In my judgment, they were not germane. And he did suggest at that time that he wanted to offer an amendment on the Senate floor. As I said, I am not personally opposed to having a vote on the Senator's amendment as long as there is a limited time of debate. But I do think and believe others will object, and they will want to have their provisions passed. I just believe at this point

it makes sense to proceed with AGOA, the DR-CAFTA bill, and the Burma bill, and deal with how we do offsets at a future date, not right now because it just gums up too much else.

The PRESIDING OFFICER. The Senator from Oklahoma.

Mr. COBURN. Mr. President, what the chairman said is this bill is paid for. I would put forward to the American public that if they went to Wendy's this afternoon and said: Give me a double cheeseburger; and, oh, by the way, over the next 10 years I am going to pay for it, most Americans would not say it is paid for.

What we are doing with this bill is taking custom user fees in the years 2021, 2020, 2019, and all the way down to pay for this bill. That is the problem. We will never solve our other problems until we get out of the mindset of saying because of the rules, we can stretch out the payment and call it paid for.

This bill isn't paid for. It is going to be paid for by the people who import things 10 years from now, not now. That is the whole point. That is why we have a \$1.3 trillion deficit this year. That is why we have at least 2 to 3 million people unemployed in this country—because of our debt. So the question is, Is there a point in time when we are going to stop paying for things in the future and pay for them now? That is my objection.

I am fully open to passing this bill if somebody will just pay for it this year. If we are not going to pay for it this year, then we are not going to pass a bill by unanimous consent.

I will tell you, nobody else operates this way. Nobody rationalizes that you can pay—and the other thing, this is just \$200 million. To everybody outside of Washington that is one ton of money. Here it is peanuts. To say we can't pay for something worth \$200 million in a bill to do this, right now, to start the self-discipline of paying for it, it just says we are not worthy of being here if we would not do that.

So I would love to work out a solution, but there is a time and place where we have to change the direction of how we operate. For me, this is the bill that now says to me we are going to start paying for things. And if we can't pay for a \$200 million pay-for in the same year, or at least the same 3 years we are going to actually spend it, then we are just not going to pass bills with my help.

I am not speaking for just TOM COBURN. The vast majority of Americans want us to pay for things by cutting wasteful spending. The fact that we are going to take custom user fees over 10 years to pay for this is ludicrous. Nobody in the rest of the economy can go out and say: Oh, by the way, I want to consume it now, but I will pay for it 10 years from now—in interest free. It doesn't work that way, and we ought not to be doing it.

The chairman has my utmost respect. He has a tough job, I know that, of trying to do that. I will continue to

try to work on solutions for this problem, but I am not moving from a position that we are going to pay for the things in the year in which we count them.

I yield the floor and I suggest the absence of a quorum.

The PRESIDING OFFICER (Mr. BROWN of Ohio). The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

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

Mr. LIEBERMAN. Mr. President, may I ask what the pending business is now?

The PRESIDING OFFICER. The motion to proceed on S. 3414.

Mr. LIEBERMAN. Mr. President, I rise to speak on the motion to proceed to S. 3414, which is the Cybersecurity Act of 2012.

This cloture motion has been filed that will ripen sometime tomorrow, but I think it is the hope of Members on both sides of the aisle that we can proceed to vote on the motion to proceed today. I am hopeful colleagues on both sides of the aisle will vote to proceed, because although there continues to be some disagreement about the content of this bill and different approaches taken, I don't think there is any Member of the Senate who doesn't appreciate the fact that our country is currently under cyber attack every day, our businesses are victims of cyber theft every day, with the consequential loss of billions of dollars' worth of investments and, I would say, tens of thousands of jobs going elsewhere.

So this bill is not a solution in search of a problem; it is an attempt to solve a problem. Although there may be differences still on different components of the bill, I hope everybody will join together in at least saying: Let's proceed to the debate, and let's see if we can reach a conclusion before we leave for the August break next week.

I will report in this regard that this morning there was a second meeting held of those who have been most active in supporting different legislation that deals with the cyber threat to America. Senator COLLINS and I, Senator FEINSTEIN, Senator ROCKEFELLER, Senator CARPER—who introduced the pending matter, the Cybersecurity Act of 2012—Senators HUTCHISON and CHAMBLISS were there today, Senator COATS—who introduced the so-called SECURE IT Act—and then a group of peacemakers-bridge builders, Senators KYL and WHITEHOUSE, Senator GRAHAM, Senator COONS, Senator BLUMENTHAL, and Senator COATS, again, who sits in two of the three groups, which makes him a superbridge builder.

It was a very good, substantive discussion, in which we were all fleshing out the details of the various proposals. We are seeing some areas where

I think we feel we have a real opportunity to agree and some areas where it may be more difficult, but we haven't given up. But overall, I would say this process has been very encouraging. Basically, all the leading parties in the Senate and all the Senators are around the same table talking, which is very constructive to have happen. I appreciate that. To me, it is more reason to vote to proceed.

I wish to begin by thanking the aforementioned Senators COLLINS, ROCKEFELLER, FEINSTEIN, and CARPER, who joined me in sponsoring S. 3414, which I wish to talk about a bit now in this opening statement.

I also wish to thank the majority leader, Senator REID, for seeing the cyber threat to America in all its urgency and reality last year, urging Senator COLLINS and me to go forward and work on legislation, to work across party lines to get a bill out and now to thank Senator REID for keeping his commitment to bring this bill to the floor, even though, as always, there are clearly other important issues vying for this body's attention. But, to me, there is none more important to America's security and prosperity than this topic, which is cybersecurity and the cybersecurity bill that is now pending.

I would like to make three points in my remarks to my colleagues.

First is that the danger of cyber attacks against the United States is clear, present, and growing, with enemies ranging from rival nations to cyber terrorists, to organized crime gangs, to rogue hackers sitting at computers almost anywhere around the world. The pending matter, S. 3414, Cybersecurity Act of 2012, responds directly and effectively to this danger.

Second, this bill has been a long time in coming. In this regard, I note a letter sent out by the U.S. Chamber of Commerce overnight that, I must say, I found very disappointing overall because, if I may state it affirmatively, it doesn't embrace the same spirit I see Members of the Senate embracing; that although we have different positions, we can't afford to be inflexible. We can't be closed to compromise because of the urgency of the threat to our country and because of the general principle that has not been as evident in the Senate and Congress generally as it should be in recent years; that we never get anything done unless there is some compromise. I am not talking about compromise of principle. But if we go into every negotiation saying, I will only accept 100 percent of what I want, ultimately we are not going to get anything, if we can get 80 percent, 75 percent, 60 percent—particularly when we are dealing with a threat to the security of the United States and our prosperity as real as the cyber threat.

I hope our friends at the Chamber will reconsider the tone of their opposition and come to the table to talk with us about their concerns and see if we can't reach common ground because

there is a larger national interest at stake than represented by any particular group or any individual Senator or their point of view.

In their letter of July 25, 2012, signed by R. Bruce Josten, executive VP for government affairs of the U.S. Chamber of Commerce, the Chamber says that:

... S. 3414, the "Cybersecurity Act of 2012," which has been rushed to the floor without a legislative hearing or markup. The bill was introduced just last week and remains a moving target; new and modified provisions of the bill are expected to be released in the coming days.

If they are, it is going to be a result of the give-and-take compromise that leads to legislation that is going on now. But I wish to respond to the idea that this came out of nowhere.

This bill has been a long time in coming. As a matter of fact, I went back and looked at the records. I attended my first hearing on cybersecurity as a member of the former Senate Governmental Affairs Committee—the predecessor to the current Homeland Security Governmental Affairs Committee—under the leadership of then-Chairman Fred Thompson. That was back in 1998, 14 years ago. I have been concerned ever since about the growing threat of cyber attack.

Along with my dear friend and colleague on the committee, Senator COLLINS, our committee has held multiple hearings on cybersecurity; that is, the new Homeland Security and Governmental Affairs Committee, and we weren't alone. There have been numerous hearings over the past several years and markups by multiple committees in both the Senate—many held by our colleagues Senator ROCKEFELLER and Senator FEINSTEIN in the Commerce and Senate Intel Committees—as well as in the House. Those deliberations and discussions were informed by numerous government and private sector studies on the dangers that lurk in cyberspace.

So this bill didn't come out of nowhere. We reported a bill out of our committee, with a lot of hearings and an open markup. We began, at the majority leader's direction, to negotiate with the other committees, particularly Commerce and Intel. We reached agreement, which is essentially what this bill is.

Incidentally, we then altered this bill—Senators COLLINS, FEINSTEIN, ROCKEFELLER, and I, in response to the bipartisan Kyl-Whitehouse group recommendations—to make it nonmandatory but still significant. So this bill has been aired and worked on and is ready for action.

But more to the point, the Senate needs to act. That is why it is so important we adopt the motion to proceed, because this threat is real, dangerous, and growing every day.

Third, this bill, S. 3414, is the result of bipartisan compromise. It is both bipartisan and it is the result of compromise. We cosponsors, as I men-

tioned, gave up some elements we thought were important that we had in our original bill. Given the cyber threat, we actually thought it was more important to move forward with a bill that will significantly strengthen our cybersecurity, even though it doesn't do everything we want it to do and thought should be done.

We didn't want to lose the chance to pass cyber legislation this year that could prevent a cyber 9/11 attack against the United States before it happens, instead of rushing in the midst of mayhem back to the Senate and House to adopt cybersecurity legislation after we suffer a major attack.

As I said, we have incorporated ideas from Senators WHITEHOUSE, KYL, and the other Members whom we were working with quite diligently to help us find common ground. I wish to explicitly and enthusiastically thank them for their efforts.

We have heard and responded to Senators DURBIN, FRANKEN, WYDEN, and others, and advocacy groups across the political spectrum from left to right, who have pressed for greater protections for privacy, personal privacy in this bill. We have made substantial changes designed to address concerns from stakeholders and colleagues.

I am confident we can work through more issues as we debate the bill on the floor. But the main point here, if I may use quite a familiar expression around here with a slightly unique follow-on phrase, I hope: If in our quest for cybersecurity legislation we allow the perfect to be the enemy of the good, we are going to end up allowing our enemies to destroy a lot that is good in the United States of America. We have to act together for the good of the Nation, get the debate started and bring amendments to the floor for an up-or-down vote.

Let me stress at this point that Senator REID, the majority leader, has been quite clear that his desire, his intention is to have the process be an open amendment process so long as the amendments are germane and relevant to the topic of the bill, cybersecurity, not just open to any amendment about any subject.

I want to go back over these three points and talk about them in a bit more detail. Let me start with the reality of the threat. I want to read from a letter sent to us recently by some of our Nation's most experienced security leaders from both Republican and Democratic administrations. Here is a letter to the majority and minority leader, signed by former Bush administration Secretary of Homeland Security Michael Chertoff; former Bush administration Director of National Intelligence ADM Mike McConnell; former Bush Deputy Defense Secretary Paul Wolfowitz; former NSA and CIA Director General Michael Hayden; former vice chair of the Joint Chiefs of Staff Marine Gen. Jim Cartwright; and former Deputy Defense Secretary William Lynn. I quote from the letter. It

is quite an impressive group, clearly bipartisan—nonpartisan.

We write to urge you to bring cybersecurity legislation to the floor as soon as possible. Given the time left in this legislative session and the upcoming election this fall, we are concerned that the window of opportunity to pass legislation that is in our view critically necessary to protect our national and economic security is quickly disappearing.

These security leaders went on to say:

Infrastructure that controls our electricity, water and sewer, nuclear plants, communications backbone, energy pipelines and financial networks must be required to meet appropriate cybersecurity standards. We carry the burden of knowing—

It is really chilling.

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

That is not a statement from a Member of the Senate or an advocate on one side or the other. These are proven national security leaders who have worked in administrations of both political parties. “It is not a question of whether a cyberattack will happen,” they say, “but when.”

Many others have issued similar warnings. Secretary of Defense Panetta has said the next Pearl Harbor-like attack against America will be launched from cyberspace.

Chairman of the Joint Chiefs of Staff Gen. Martin Dempsey has warned: “A cyberattack could stop our society in its tracks.”

Just this month, National Security Agency Cybercommand Chief Gen. Keith Alexander blamed cyber attacks for: “The greatest transfer of wealth in history.”

General Alexander estimated that American companies lose about \$250 billion a year through intellectual property theft through cyberspace; \$114 billion to theft through cyber crime; and another \$224 billion in downtime the thefts caused.

We talk a lot here in the Senate these days, as we must, about how we protect American jobs. It turns out that in creating more cybersecurity in our country we are also going to protect tens of thousands of jobs which otherwise are going to end up elsewhere in the world because they will have stolen the industrial secrets that lead to the new industries that create those jobs.

General Alexander concluded this part of the statement he made by saying: “. . . this is our future disappearing before us.”

Cyber attack.

These fears are not speculative. Let me go through a recent op-ed in the Wall Street Journal that President Obama wrote.

In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home. Taking down vital

banking systems could trigger a financial crisis. The lack of clean water or functioning hospitals could spark a public health emergency. And as we have seen in past black-outs—

Which were caused by natural disasters, for instance—

the loss of electricity can bring businesses, cities and entire regions to a standstill.

These fears are not speculative. They are not theoretical. They are based on existing facts and existing vulnerabilities. Consider, if you will, this recent story in the Washington Post that detailed how a young man living an ocean away used his computer to hack into the control panel of a small town water utility in Texas. It took him just 10 minutes and required no special tools or training. The utility had no idea of what had happened until the hacker posted screen shots of his exploit online as a warning of how vulnerable all of us are. Imagine if terrorists decided to target a string of small utilities across the United States and either cut off fresh water or dumped raw sewage into our lakes, rivers, and streams. We would have an environmental and economic disaster on our hands. But this is a real possibility.

This brings me to my second point. We need to act and act now. The challenge of cybersecurity has been studied for a long time and there is no need for more studies or hearings or delay, as the Chamber letter requests. I went back to the Congressional Research Service. According to a report that they issued, in the 112th Congress alone there have been 38 hearings and 4 markups in the House and 33 hearings in the Senate on cybersecurity.

In the 112th Congress, the Judiciary Committee also held a markup on the Personal Data and Privacy Security Act and in previous Congresses the Senate has held markups on cybersecurity legislation in five separate committees under regular order, all of which is included in the bill that is pending before us today.

Since 2005, the Senate Homeland Security Committee alone has held 10 hearings with 48 witnesses testifying and took questions over a total of 18 hours. Look at the bill’s cosponsors. S. 3414: Senators COLLINS and I, along with Senators FEINSTEIN and ROCKEFELLER, have held numerous hearings, forums, and cybersecurity demonstrations for Members and staff. All these hearings and briefings were further informed by, according to the CRS, a total of 60 governmental reports totaling 2,624 pages produced by the GAO, the Department of Defense, the OMB, the Department of Energy, and other Federal agencies. This doesn’t count the many more reports from the private sector—computer security firms such as SEMANTEC and think tanks and academic institutions such as MIT and the Center for Strategic and International Studies.

This matter is ready for action. I go back to a 1936 book Winston Churchill wrote, “When England Slept.” Not

“Why England Slept” but “When England Slept”. He asked his colleagues in the Parliament who were refusing at that time to act decisively to counter the rise of German military power despite its clear threat to Europe—Churchill said: “What will you know in a few weeks about this matter that you do not know now . . . and have been not been told any time in the last six months?”

I think the same can be said now. That is why I think it is so important to adopt the motion to proceed and get something done before we leave Washington for the August break.

Finally, in the interest of moving forward, my cosponsors and I, as I indicated earlier, have made a major compromise in the bill we are bringing to the floor in terms of how we deal with critical cyber infrastructure. Here again, we are talking not about small businesses around America, we are talking about powerplants, energy pipelines, water systems, financial systems that we all depend on for our banking, water—sewer systems, for instance—that if sabotaged or commandeered in a cyber attack could lead to catastrophic deaths and economic and environmental losses.

In our original bill, Senators COLLINS, FEINSTEIN, ROCKEFELLER, and I called for mandatory cyber safety standards for all critical infrastructure after those standards were developed in consultation with the private sector. We did not think this was a unique or onerous requirement but our responsibility in carrying out our constitutional oath to provide for the common defense. Since antiquity, as a matter of fact long before the American Constitution, societies have chosen to adopt safety standards to protect their citizens, particularly safety standards for physical structures starting with the homes we live in, but also our offices, factories, and critical infrastructure such as powerplants and dams. Today we call these building codes. Can you imagine if there were no building codes, the danger that people would take when they walked in our office buildings or factories or apartment houses or residences?

I cannot resist saying these building codes in some sense are as old as the Bible. Here I go to Deuteronomy 22:8 which says:

When you build a new house, you shall build a parapet for your roof, so you shall not bring the guilt of blood upon your house if anyone should fall from it.

There is direct relevance in a very different context from the Biblical context to what we are trying to do here, which is to build a kind of parapet around our cyber systems so we do not bring the guilt of blood on us because somebody has attacked through those cyber systems.

The reason we have done this over antiquity in the physical world is obvious. If one of our homes catches fire because of the wiring not up to code or it happens in an apartment building or an

office building, the people in it are endangered, obviously, but also the lives and homes of our neighbors, the community are in danger as well. Numerous bipartisan national security experts have been in total agreement that mandatory requirements are needed to protect our national and economic security from the ever-rising risk of cyber attacks.

But it was this provision, seen in the context of regulation of business while we were seeing it as homeland security, protecting homeland security, that was the most controversial in our compromise bill and drew the most criticism. To be more specific about it, it threatened to prevent passage of any cybersecurity legislation this year which, for the sponsors of this bill, was simply an unacceptable result.

Following the rule that no matter how deeply one believes in the rightness of a provision in a bill, we agreed to change it because there is so much else that is critically important in our bill that will protect America's cybersecurity. So we withdrew the mandatory provision and created all the standards for performance of how the most critical infrastructure, cyber structure, would protect itself. But then we left it voluntary; however, we did create some incentives. Let me be clear that the decision is to be what we all want it to be, which is as a result of a collaborative, cooperative effort that businesses that operate the most critical cyber structure, such as, electrical systems, water systems, transportation, finance, communications, will want to comply.

Under our revised bill, private industry, which incidentally owns as much as 85 percent of the Nation's critical infrastructure—that is the American way, and that is great. But when that 80 to 85 percent of our critical infrastructure can well and probably will be the target of not just theft but attacks by enemies of the United States, we have to work together to prevent that.

In our bill we give the private sector the opportunity to develop a set of cybersecurity practices which will then be reviewed by the new National Cybersecurity Council that our bill creates. It will be chaired by the Secretary of Homeland Security and made up of representatives of the Department of Defense, Commerce, Justice, and the intelligence community, and presumably the Director of National Intelligence. This National Cybersecurity Council will review the standards agreed upon by the private sector and decide whether they are adequate to provide the necessary level of cybersecurity for the American people.

Owners of critical infrastructure will then have a decision to make. Do they want to essentially opt into the system or do they want to not do so? That is up to them under the bill as is put before them because it is voluntary. If they opt in—and this is what we hope will be an incentive—they will be entitled to receive some benefits, the most

significant of which will be immunity from certain forms of liability in case of a cyber attack. We also offer expedited security clearances and prioritize technical assistance from our government on cyber questions from those critical covered cyber-infrastructure companies that opt into the system.

I think our colleague from Rhode Island, Senator WHITEHOUSE, has a very good metaphor for what we are trying to do. As he said, we are trying to build Fort Cybersecurity where we essentially become part of a system that provides greatly enhanced protection from cyber attack and cyber theft, but we are not compelling anybody to come into Fort Cybersecurity. We are encouraging them to do so, and we are giving them some incentives to do so. Of course, we hope that sound and wise administrators of those companies and forces of the marketplace will encourage them to make a decision to come into Fort Cybersecurity.

Finally, our bill contains information-sharing provisions, which I think most people who have looked at the threat of cyber attack and cyber theft think are very important. These provisions will allow the private sector and government to share threat information between each other and among themselves. In other words, one private company can share information about an attack with another private company to see if the attack is part of a broader pattern.

For instance, they can talk about where it may be coming from to raise their cyber defenses against it, and to do so without fear of—well, for instance, any trust action by the State or Federal Government. Also, very often companies that believe they have been a victim of cyber attack will go to the Federal Government, the Department of Homeland Security, or the National Security Administration for help; however, a lot of them don't. Part of the reason for that is they fear, among other things, they may compromise the privacy of their records. Others, quite frankly, don't want to admit they have been attacked. This is a real problem. I will come back to that in just a moment.

We give protection from liability for companies that share their information with the government. Yet there were many individual Senators and many people from outside groups who are focused on privacy who were concerned that in doing this we were opening up a method by which parts of our Federal Government could basically violate privacy restrictions, take personal information off of the information shared by a private company with the government, and they be the victim of some kind of public intrusion or even law enforcement.

So I think we negotiated a good series of agreements on this which, one, will ensure that companies who share cybersecurity information with the government give it directly to civilian agencies and not to military agencies. That was a concern people had.

Second, we ensure that information shared under the program be reasonably necessary and described as a cybersecurity threat. In other words, not just wantonly share it because some of this is private information.

Third, we restrict the government's use of information it receives under the cyber information-sharing authority so that it can be used only for actual cybersecurity purposes and to prosecute cyber crimes with two exceptions broadly agreed on: One is that the information can be used to protect people from imminent threat of death or physical harm; and, two, to protect children from serious threats of one sort or another.

Next, we would require annual reports from the Justice Department, Homeland Security, the defense and intelligence community, and inspectors general to describe what information has been received in the previous year, such as, who got it and what was done with it. Finally, we allow individuals to sue our government if the government intentionally or willfully violates the law; that is to say, the law relating to these privacy protections.

I am very pleased by these changes we made. I want to say this loudly and clearly: This bill is about cybersecurity. But in trying to elevate our cybersecurity, we didn't want to compromise people's privacy or their freedom. So what I have just read was intended to assure that this bill, as best we could, would not compromise privacy or freedom rights.

Then I took this set of compromises to the most important people in our government who are focused on cybersecurity—the Department of Homeland Security, the National Security Agency, the FBI—and they all said, I am pleased to say, these privacy protections will not inhibit their ability to protect America's cybersecurity. They can live with these without the slightest diminishing of their focus, which understandably is not privacy but it is cybersecurity. They said these amendments to our original bill don't inhibit what they are doing.

I conclude by, again, urging my colleagues to vote, presumably today, yes on the motion to proceed so we can get the debate started, so we can continue to work to achieve common ground and a meeting of the minds and enact this piece of crucial national and economic and security legislation in this session of Congress.

I thank the Chair, and I yield the floor.

The PRESIDING OFFICER. The senior Senator from Texas.

Mrs. HUTCHISON. Mr. President, I have listened to the distinguished Senator and chairman of the Homeland Security Committee and the presentation of the bill that I assume will be voted on today. I appreciate very much that we have had the meetings. There are really two bills that have been introduced: the Lieberman-Collins, bill with their cosponsors, and then I have introduced legislation called the SECURE

IT Act along with Senators MCCAIN, CHAMBLISS, GRASSLEY, MURKOWSKI, COATS, JOHNSON, and BURR. These are eight ranking members of committees and subcommittees who have jurisdiction over cybersecurity, and we differ in a major way from the bill that is before us that is cosponsored by the Chair and ranking member of the Homeland Security Committee. All the other ranking members of the committees that have jurisdiction, are in disagreement with their approach.

Now, the good news is we have been meeting to try to begin to work out the differences and see if we can move forward. Our bill, the SECURE IT bill, will be introduced as an amendment in the nature of a substitute if, in fact, we take up the bill today.

I would agree with what Senator LIEBERMAN said right off the bat in that I believe, as long as we have an open amendment process, we will vote to move to the bill. I don't think anyone in our group or anyone with whom I have talked wants to hold up dealing with cybersecurity. We know America's systems could be under threat, and some have been hacked into already. There are terrorists who seek to sabotage networks. There are people who want access to proprietary information and intellectual property. We need to protect our systems and our country against those attacks, which is why as long as we have an amendment process and we are not shut out from discussing this, we will vote to move forward to the bill.

This bill was not marked up in committee. It did have a lot of hearings in committee. Since it wasn't marked up, amendments were not able to be introduced and discussed and voted on, which makes it harder, as we all know, when we come to the floor with a bill where there are major disagreements. We have not had the capability for the committee to take up the amendments and vote on them. That is why I think we need to have the open amendment process and why we do want to move forward on the good faith that it will be open.

Now, our bill, the SECURE IT Act, is centered on consensus items. It sets aside the controversial provisions that are of questionable need, and it is also one that we believe we can work with the House on to pass and send to the President. The bill we have would greatly improve information sharing to and from and with the government with other private sector industries in the same field, and we think that is the most important step we could all take on a fairly quick basis to start the process of getting more security throughout our systems.

We must also ensure that the entities and government and industry share information back and forth. It has to be a two-way street. Obviously, if an industry is going to share information about potential threats, if they see risks or they see problems in a system, it must get information from the gov-

ernment agencies that are doing the intelligence gathering on a quick basis.

Our bill also dramatically improves cybersecurity for Federal agencies themselves. It does update the rules that govern cybersecurity, and it requires any government contractor to inform their agency clients if their clients' systems are under a significant risk or attack. We think that is reasonable as a part of a government contracting requirement.

Today antitrust laws and liability concerns inhibit private companies from exchanging the information that is necessary to defend against and respond to cyber threats. If a company is going to be encouraged to share information with a competitor about cyber threats, they have to know they are not going to be then hit with an antitrust lawsuit. I think that is pretty clear. So our bill does address that. We make it very clear there are antitrust immunities as well as most certainly immunity from a lawsuit if they provide information on a voluntary basis. If they are sued, and they have acted in accordance with our bill, then they would have protection from liability for a lawsuit on cyber attack. So those are the things we do that I think will open up the information sharing, which is the way we believe it is important as the next step.

It is also very important that we have the safeguards for privacy. I do believe the underlying bill certainly protects privacy, and so does our substitute. We have safeguards that protect the privacy and civil liberties of all Americans while we preserve the right to ensure that we try to protect America in general from attack from the outside.

We also in our bill improve the security of Federal information systems and facilitate the prosecution of cyber crime. We want to beef up protections against criminals who are hacking in, as well as potential terrorists who might, in order to be able to prosecute against cyber crime as a disincentive to break the law.

Finally, our legislation has broad industry support. The businesses in the private sector that know their systems best and that fight every day to protect their systems and networks believe SECURE IT is the best way to go. We believe that with the cooperation of the business community, without having a big regulatory morass, is the way we are going to get the most cooperation from the people who are running the networks and systems.

I have letters of endorsement from the U.S. Chamber of Commerce, the National Association of Manufacturers, the American Fuel and Petrochemical Manufacturers, the American Petroleum Institute, U.S. Telecom, National Retail Federation, the Internet Security Alliance, and I ask unanimous consent that these letters be printed in the RECORD.

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

CHAMBER OF COMMERCE OF THE
UNITED STATES OF AMERICA,
Washington, DC, June 29, 2012.

Hon. JOHN MCCAIN,
U.S. Senate,
Washington, DC.

Hon. KAY BAILEY HUTCHISON,
U.S. Senate,
Washington, DC.

DEAR SENATORS MCCAIN AND HUTCHISON: The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than three million businesses and organizations of every size, sector, and region, supports S. 3342, the "SECURE IT Act of 2012." This bill would dramatically help the United States improve its cybersecurity posture and serve as a catalyst for greater sharing of targeted cyber threat information between the government and the private sector.

The Chamber agrees that the right path forward is for the public and private sectors to work together in solving mutual challenges, increasing real-time cyber threat information sharing between and among the public and private sectors, and fostering the development and deployment of innovative cybersecurity technologies. This path provides the best opportunity of staying ahead of fast-paced cyber threats.

The Chamber also agrees that Congress should not layer additional cybersecurity regulations on the business community. New compliance mandates would automatically drive up costs and misallocate business resources in a tough economy without necessarily increasing security. Critical infrastructure owners and operators already devote significant resources toward protecting and making their information systems more resilient because it is in their overwhelming interest to do so and good for the country.

Another positive aspect of S. 3342 is that it would leverage existing information-sharing and analysis organizations and incorporate lessons learned from pilot programs undertaken by critical infrastructure sectors. Both offer complementary, demonstrated models to enable the government to share cyber threat information with the private sector in a trusted, constructive, and actionable manner without creating burdensome regulatory mandates or new bureaucracies.

S. 3342 would also provide businesses the much-needed certainty that threat and vulnerability information shared with the government would be provided safe harbor and not lead to frivolous lawsuits, would be exempt from public disclosure, and would not be used by officials to regulate other activities. The Chamber welcomes your efforts to make certain that the information-sharing processes in your bill include necessary privacy and civil liberties protections, such as tightening the definition of cyber threat information.

The Chamber appreciates your efforts to address an array of industry concerns. As the SECURE IT Act progresses, we look forward to working with you to tailor the scope of information that certain entities in the private sector could be required to provide a government agency or department under statute.

Equally, we want to ensure that government entities continue to acquire the most innovative and secure technology products and services under provisions of S. 3342 related to reforming the Federal Information Security Management Act. Federal officials who manage agencies' information security programs should leverage industry-led, globally accepted standards for security assurance during the acquisition process. Added language stipulating that the bill would not convey any new regulatory authority to agencies or departments is a step in the right direction.

The Chamber believes that your bill highlights the notion that Congress should focus on enacting legislation that would truly improve the sharing of actionable and targeted information between public and private entities in order to defeat our mutual adversaries—not layering additional regulations on the business community. We appreciate your commitment to a nonregulatory approach to bolstering collective security; it is one that the Chamber strongly supports.

Sincerely,

R. BRUCE JOSTEN.

NATIONAL ASSOCIATION OF
MANUFACTURERS,
Washington, DC, March 26, 2012.

Hon. JOHN MCCAIN,
U.S. Senate,
Washington, DC.

Hon. KAY BAILEY HUTCHISON,
U.S. Senate,
Washington DC.

DEAR SENATOR MCCAIN AND SENATOR HUTCHISON: On behalf of the 12,000 members of the National Association of Manufacturers (NAM), the largest manufacturing association in the United States representing manufacturers in every industrial sector and in all 50 states, I am writing to express the NAM's support for S. 2151, the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act or "SECURE IT" Act.

Manufacturers through their comprehensive and connected relationships with customers, vendors, suppliers, and governments are entrusted with vast amounts of data. They hold the responsibility of securing this data, the networks on which it runs, and the facilities and machinery they control at the highest priority level. Manufacturers know the economic security of the United States is directly related to our cybersecurity.

The NAM supports the government sharing timely and actionable threat and vulnerability information with the private sector. We also support the creation of a voluntary framework that allows companies to share information with the government and with each other without creating new liabilities.

NAM member companies also support allowing the private sector to continue developing appropriate general and industry-specific best practices in collaboration with the Federal government for improved security. Encouraging manufacturers to adopt industry-standard best practices through incentives is the best way to ensure innovation while addressing the evolving threats to our nation's security. In contrast, mandates on the use of specific technologies or standards and imposing a prescriptive regulatory framework would unduly inhibit innovation.

The SECURE IT Act addresses these issues important to manufacturers. The bill would allow for voluntary information sharing across the cyber community and protect information owners from liability stemming from those actions. It would also help secure government networks, increase the penalties for cybercrime, and prioritize cybersecurity research using existing government dollars. The SECURE IT Act does this without creating a new and unnecessary regulatory burden on manufacturers.

The NAM and all manufacturers remain intensely committed to working with Congress to secure our cyberinfrastructure from harm. We look forward to thoughtful discussions and examination by all the Committees with jurisdiction on this issue to ensure that any legislation that moves forward mitigates the cyber threat facing our nation.

Sincerely,

BRIAN J. RAYMOND,
Director, Technology Policy.

AMERICAN FUEL & PETROCHEMICAL
MANUFACTURERS,
Washington, DC, March 13, 2012.

Re AFPM supports the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act.

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

DEAR SENATORS REID AND MCCONNELL: AFPM, the American Fuel and Petrochemical Manufacturers (formerly National Petrochemical & Refiners Association), writes today to express its support for S. 2151, the "Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act of 2012" introduced by Senators McCain, Hutchison, Grassley, Chambliss, Murkowski, and Coats. This important legislation breaks down current barriers to information sharing to ensure greater security without interfering in the ability of private-sector businesses to protect their own IT systems.

AFPM is a trade association representing high-tech American manufacturers of virtually the entire U.S. supply of gasoline, diesel, jet fuel, other fuels and home heating oil, as well as the petrochemicals used as building blocks for thousands of products vital to everyday life. Protection of our members' Information Technology (IT) and Industrial Control Systems (ICS) are critical to the fuel and petrochemical manufacturing process.

The SECURE IT Act opens avenues to foster greater information sharing between the private sector, non-federal government agencies, and Federal cybersecurity centers, allowing private companies to voluntarily share information without concern of anti-trust and liability violations. Instead of creating a massive regulatory regime under the Department of Homeland Security, this legislation recognizes the proactive role the refining and petrochemical industries have taken to protect our facilities. The sharing of information among companies, as well as with the federal government, will improve our preparedness for an attack and better educate our companies' employees on the various threats facing all critical infrastructures.

AFPM's members remain concerned over alternative approaches to cybersecurity that would create an environment focused simply of compliance with bureaucratic government regulation, rather than on actual security. Because cyber threats and crimes are always changing, establishing a one size fits all regulatory framework for our facilities could create more vulnerabilities and has the potential to make existing cybersecurity protections significantly less effective.

Cybersecurity is critical to protecting refineries and petrochemical facilities. Breaking down the barriers to information sharing will ensure our security and provide our facilities with timely information to better protect our systems against attack. AFPM believes that the SECURE IT Act will make America and its IT and ICS systems more secure and urges your support for this legislation.

Sincerely,

CHARLES T. DREVNA,
President, AFPM.

API,

Washington, DC, March 7, 2012.

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

DEAR SENATORS REID AND MCCONNELL: We are writing to express our support for S. 2151 "SECURE IT Act of 2012", which was recently introduced by Senators McCain, Hutchison, Chambliss, Grassley, Murkowski, Coats, Burr and Ron Johnson. The American Petroleum Institute is the national trade organization representing nearly 500 companies involved in all aspects of the domestic oil and natural gas industry.

We appreciate the balanced and carefully crafted approach taken in S. 2151, using and improving upon sector-based cybersecurity processes and partnerships already in progress, and working toward increased collaboration between government and industry rather than imposing additional and unworkable regulations. For example, the sharing of timely and actionable information on cyber threats, vulnerabilities and mitigation procedures will help companies improve their detection, prevention, mitigation and response capabilities. Continuing to improve valuable information sharing, both between a company and the government and among companies within industry sectors, is an effective tool in advancing our nation's cybersecurity.

We remain concerned that alternative legislative approaches under consideration could have unintended consequences on business and industry, including the diversion of resources away from activities that will reduce or mitigate risks associated with daily cyber threats in order to comply with mandates that would soon be outdated.

Cyber threats change rapidly. API believes the proposed path to improved information sharing will encourage the public and private sectors to work together to reduce risk and promote investment in new technologies to keep industry cyber systems secure. Legislation must enhance, rather than impede, innovative processes and encourage advancements in new cyber risk assessment and mitigation measures.

API recognizes the leadership of the "SECURE IT Act" sponsors in addressing our nation's cyber security challenges. We appreciate the continued commitment to offer valuable solutions on this complex issue and look forward to working together in the days and weeks ahead.

Sincerely,

MARTY DURBIN,
Executive Vice President.

NATIONAL RETAIL FEDERATION,
Washington, DC, June 27, 2012.

Hon. JOHN S. MCCAIN,
U.S. Senate, Russell Senate Office Building,
Washington, DC.

DEAR SENATOR MCCAIN: The National Retail Federation strongly supports your efforts to craft effective cybersecurity legislation to protect our nation's critical infrastructure from cyber-attacks and we appreciate and applaud your introduction today, June 27, of S. 3342, the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012 (the "SECURE IT Act"). In your efforts to develop a bipartisan bill for Senate floor consideration, we urge you and your co-sponsors to ensure that all provisions of the bill support the overall purpose of protecting our critical infrastructure and are not expanded to include unrelated or unvetted amendments, such as data breach and commercial privacy legislation.

As the world's largest retail trade association and the voice of retail worldwide, NRF represents retailers of all types and sizes, including chain restaurants and industry partners, from the United States and more than 45 countries abroad. Retailers operate more than 3.6 million U.S. establishments that support one in four U.S. jobs—42 million working Americans. Contributing \$2.5 trillion to annual GDP, retail is a daily barometer for the nation's economy. NRF's Retail Means Jobs campaign emphasizes the economic importance of retail and encourages policymakers to support a Jobs, Innovation and Consumer Value Agenda aimed at boosting economic growth and job creation.

The SECURE IT Act advances the important goal of facilitating cooperative information sharing about cyber threats between the government and private sector, a key component of cybersecurity legislation we support. The goals underlying cybersecurity legislation and provisions in data breach notification legislation are fundamentally contradictory. The cybersecurity proposals encourage information sharing by limiting companies' liability for that sharing. On the other hand, some proposed breach notification bills either penalize companies for sharing news of a breach, by imposing onerous credit monitoring obligations, or impose lesser civil penalties for failing to disclose a breach in the first instance. Juxtaposing these contrasting proposals would place businesses in a precarious position when their systems are attacked by cyber criminals. Thoughtful examination and comparison of the SECURE IT Act with proposed data breach legislation reveal that they are not properly aligned.

A similar case exists with respect to commercial privacy legislation called for by the Obama Administration in its Privacy and Innovation Blueprint and by the Federal Trade Commission in its final privacy report. Comprehensive consumer privacy legislation, which has not been vetted by any committees of jurisdiction in the Senate, attached to the SECURE IT Act, flies in the face of the deliberative process that this sensitive topic deserves.

Congress must strike the careful balance between consumers' privacy interests and the provision of goods and services over the Internet that the average American consumer expects in this e-commerce economy. That type of careful deliberation, we fear, may not take place on the Senate floor at this time. Furthermore, these commercial privacy provisions are unrelated to the core purposes of cybersecurity legislation, and Congress has ample time to fully consider the positions and concerns of all stakeholders in a separate and unrushed legislative process.

NRF is supportive of your efforts to create a cybersecurity bill that is based on fully vetted concepts that will aid in protecting our nation's most critical infrastructure but that is not encumbered with conflicting amendments addressing data breach notification or insufficiently examined new privacy regimes. NRF looks forward to working with you on this legislation moving forward.

Sincerely,

DAVID FRENCH,

Senior Vice President, Government Relations.

Mrs. HUTCHISON. Mr. President, our bill also allows for a true collaborative effort.

The reason we are not supporting the bill that is on the floor today is because we believe it does not do the priorities that we can pass, and it does increase the mandates and the regulatory overkill, in our opinion, that

will keep our companies from being able to move forward on an expedited basis to start protecting our systems.

A priority of mine throughout this process has been that we help the private sector combat cyber attacks by breaking down the barriers to sharing information. If we could take that one step, we would be a long way toward ensuring that we are increasing the security of all Americans. The bill before us will actually undermine current information sharing between the government and the private sector. That bill's information-sharing title is a step backward because it slows the transfer of critical information to our intelligence agencies, and there is not sufficient protection from antitrust. In addition, there is no consensus in the Senate to grant the Department of Homeland Security broad new authority to impose burdensome regulations on the private sector.

While I am pleased our colleagues who are cosponsoring the bill that is before us have made an effort to move away from direct regulation of our Nation's systems, it has a long way to go. While their bill allows the private sector to propose standards that are described as voluntary, the bill actually empowers Federal agencies to make these voluntary standards mandatory. If an agency does not make the standards mandatory, it would have to report to Congress why it had failed to do so. That is a pretty big incentive for mandates to start being put on with regulations that will be required.

I believe there is a way forward. If the Senate takes the well-reasoned and broadly supported provisions of the SECURE IT bill and puts them with a voluntary and industry-driven critical infrastructure protection title, we could pass a Senate bill with overwhelming support.

The key to reaching consensus has five parts:

The cybersecurity standards must be developed by the private sector and must be truly voluntary. The relationship between government and the private sector in this area must be cooperative, not adversarial and not regulatory.

The National Institute for Standards and Technology should be the convening authority for the private sector standard-setting process. The government can have a role in ensuring the standards are sufficient, and it should, but it can't establish a regulatory regime that will lengthen and hamper the efforts to open information sharing.

Companies—and here is the incentive for the companies to do exactly what we are asking them to do—companies that adopt the voluntary standards must receive robust and straightforward protections from liability as well as necessary antitrust and Freedom of Information Act exemptions. If a company is going to turn over its proprietary information to the government, it must be protected from free-

dom of information requests from the government that then would take its private proprietary information public.

As in the SECURE IT Act, the information-sharing title must be strong and encourage the private sector to share information, and it must encourage the government to share with the private sector. It cannot cut out those with the most expertise in the area, meaning the national security agencies should not have to be subservient to the Department of Homeland Security.

In addition, a 5-year sunset would allow Congress to revisit the act and make needed changes. FISA has certainly shown that with a sunset, it allows the flexibility to adapt to new issues that arise and stay current in its processes to deal with cybersecurity. We believe a 5-year sunset would be the right amount of time to get this going, set things in place, see what works, and see what needs to be adjusted.

I am hopeful my colleagues and I can come to a compromise on this critical issue. We want a strong cybersecurity bill. We want one that can pass both Houses. The five points I have laid out could get us to a bill that will significantly take the steps to improve our Nation's cybersecurity.

I wish to read a couple of excerpts from the Heritage Foundation's views of the bill that is before us today:

Cybersecurity legislation will likely be taken up by the Senate tomorrow.

This was written yesterday.

Regrettably, the idea that we just need to do something about cybersecurity seems to be trumping the view that we need to do it right.

The Cybersecurity Act of 2012, authored by Senators Lieberman and Collins, seeks to solve our cybersecurity ills but only threatens to make the situation worse.

The "voluntary" nature of the CSA's standards is also questionable. Any voluntary standard is one step away from mandatory, and Senator Lieberman has already indicated that if the standards aren't voluntarily used, he would push to make them mandatory.

Even more concerning, section 103(g) of the CSA gives current regulators the power to make these "voluntary" standards mandatory.

It specifically authorizes that action.

If a regulator doesn't mandate the standards, the regulatory agency will have to report to Congress why it didn't do so.

Again, there is strong encouragement to just make the standards mandatory and avoid a congressional inquisition.

Finally, the Heritage Foundation goes on to say:

Finally, the sharing and analysis of cybersecurity threat information was weakened by confining cybersecurity information exchanges to civilian organizations. Though in an ideal world the Department of Homeland Security would have the capability to lead our cybersecurity efforts, it currently lacks those capabilities and needs to lean on more capable organizations such as the National Security Agency. The recent changes, however, give DHS more responsibility than it is likely able to handle.

So we will certainly move forward with the understanding that we will

have the ability to offer amendments and try to make this a workable bill. It is certain that because the committee was not able to mark up the bill, we have to have the amendments to try to perfect it.

I would very much like to take the first step forward in cybersecurity, which is why, assuming we have the right to amend, I will support going to the legislation so that we can start the amendment process next week. I think the people who are cosponsors of my legislation, along with Senator MCCAIN, Senator CHAMBLISS, Senator GRASSLEY, Senator BURR, Senator MURKOWSKI, Senator COATS, and Senator JOHNSON, want to make sure we do this right. As the Heritage Foundation has so aptly said, we don't want a big, new regulatory scheme that is not going to be successful in our efforts to improve the cybersecurity safeguards in our system.

We are the ranking members of all but one of the relevant committees. We know this area. We deal with the agencies that deal with cybersecurity and all of the national security in our country. We know what can work, we know what we have a chance to pass, and we know how to take the first step forward without another big regulatory overreach, as we have seen happen in the last 3½ years in this administration. We hope to work with the majority, with the Lieberman-Collins bill, and come up with something that everyone will feel is the right step forward. We would like to have a bill that will get a large number of votes rather than a very lopsided vote against it.

I appreciate very much that we are now beginning to discuss this. I am appreciative that we have had several meetings with all of the sides that have been put forward as having concerns with the bill that is on the floor as well as its sponsors. I hope we can keep working toward a solution that will protect America and do it in the right way.

Thank you, Mr. President. I yield the floor.

THE PRESIDING OFFICER. The senior Senator from Arizona.

Mr. MCCAIN. I thank the Chair. I ask unanimous consent to take 5 minutes in morning business and then speak on the pending legislation.

THE PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

TRIBUTE TO AMBASSADOR RYAN CROCKER

Mr. MCCAIN. Mr. President, I would note that I saw my friend Senator LIEBERMAN on the floor a second ago, and I know he joins with me in this statement.

I wish to take a few minutes to pay tribute to Ambassador Ryan Crocker, who ended his tour this week as the U.S. Chief of Mission in Kabul, Afghanistan.

As some of my colleagues may know, Ambassador Crocker's health has unfortunately been poor, so he is returning to receive some much needed care.

But what my colleagues may not know is that Ambassador Crocker's health has been poor for some time and the people who care about him most—his family, his friends and colleagues in the Foreign Service, and our Secretary of State herself—told Ambassador Crocker long ago that he needed to leave his post and that he needed to get away from the long days and long nights of too much stress and not enough sleep. They told him to come home for his own sake.

Eventually, Ambassador Crocker relented, but still he was only going to leave on his own terms. He said that America asks the best of our country—our men and women in uniform and their many civilian partners who work and sacrifice shoulder to shoulder with our troops in the field—to serve in Afghanistan for 1 year. Ambassador Crocker said he would expect no less of himself, and do no less, whatever the cost. So for the past few months, Ambassador Crocker has fought through persistent pain and discomfort to finish out his 1-year in Kabul, doing everything that is asked of him—and more. On Tuesday, that year came to an end, and Ambassador Crocker came home to receive the care he desperately needs.

This is a remarkable story, but it is only surprising to those who do not know Ryan Crocker. For those of us who have had the pleasure and the honor of coming to know Ryan well, this latest story is not at all surprising. It is actually quite in keeping with the character and the actions of this superb, decent, and selfless man—a man whom I would call, without question or hesitation, the most excellent Foreign Service officer and one of the finest public servants I have ever known.

For the past 41 years, ever since he was a junior diplomat serving in prerevolution Iran, Ryan Crocker has consistently answered the call to serve in the most challenging, the most difficult, but also the most important posts in the world. They were the places, as it turned out, where America needed Ryan Crocker the most, and he has always served with distinction.

He was a young officer in Lebanon when our Embassy was bombed, and Ryan Crocker helped to pull his colleagues from the rubble and then got back to work. He was one of the first civilians into Afghanistan and Iraq after the recent wars, helping to reestablish our diplomatic presence in both countries after decades. He returned to Iraq during the surge and, as General Petraeus tells everyone, was absolutely indispensable in turning around our war effort, even as his life was constantly in danger from the rockets that smashed into his office in Baghdad and, perhaps more threatening, his own relentless work ethic, which literally almost killed him.

Many Presidents, Republicans and Democrats alike, have had the wisdom to appoint Ryan Crocker as their Ambassador to six different countries—

Lebanon, Kuwait, Syria, Pakistan, Iraq, and finally Afghanistan.

Ambassador Crocker has been just as indispensable in Kabul as he has everywhere else in his career, from enhancing our relationship with President Karzai and the people of Afghanistan, to negotiating and concluding the Strategic Partnership Agreement with Afghanistan, to being the dedicated partner every hour of every day of GEN John Allen and all of our men and women serving in harm's way.

In my many years and my many travels, I have had the pleasure and honor of meeting and getting to know many of our career diplomats, and I am continually impressed by their high quality and tough-mindedness, their patriotism and love of their country, their constant willingness to serve and the many quiet sacrifices they make. But of all of these remarkable men and women, never have I met a Foreign Service officer more outstanding or more committed to our country than Ryan Crocker.

The one comfort I take in Ryan's departure from Afghanistan is that he remains an abiding inspiration to his fellow diplomats, who revere him and hold him in the highest regard and wish to model themselves and their careers after his life and service. America will be a better and safer place because of this, thanks to Ryan Crocker.

Mr. President, I rise today to oppose the Cybersecurity Act of 2012 because it would do very little to improve our country's national security. In fact, in its present form, I believe the bill before us would do more harm to our country's economy and expand the size and influence of the Federal Government—specifically, the Department of Homeland Security—than anything else.

But before I begin my critique of the Cybersecurity Act, I would like to reaffirm my sincere respect for the lead sponsor of this bill—both sponsors, actually, both Senators LIEBERMAN and COLLINS. Although I disagree, whatever criticisms I may have with the legislation should not be interpreted as an attack on the sponsors of the bill but, rather, on the process by which the bill being debated today arrived before us and its public policy implications.

Consider this for a moment: If we pass this bill in its present form, which I hope we will not, we will have handed over one of the most technologically complex aspects of our national security to an agency with an abysmal track record, the Department of Homeland Security. The problems at DHS are too numerous to list here today, but I think I speak for many when I question the logic of putting this agency in charge of sensitive national security matters. They cannot even screen airline passengers without constant controversy. And do not forget that this is the same outfit in charge of the Chemical Facility Anti-Terrorism Standards Program, or CFATS, which was described in a recent report as “at

measurable risk," beset by deep-seated problems such as wasteful spending and a largely unqualified workforce that lacks "professionalism." I for one am not willing to take such a broad leap of faith and entrust this complex area of our national security and so many vibrant parts of our economy to this ineffective, bloated government agency.

The poor quality of the bill before us is a direct reflection of the lack of a thorough and transparent committee process. Had this bill been subjected to the proper process, my colleagues and I and the American public would have a much better understanding of the real implications of this undertaking. Unfortunately, this bill has not been the subject of one hearing, a single markup, or a whiff of regular legislative procedure.

Our Nation's cybersecurity is critical, and the issue is deserving of the regular order and the full attention and input of every Member of this body. I urge the majority leader to allow a full, fair, and open amendment process if cloture is invoked on the motion to proceed.

All of us should recognize the importance of cybersecurity. 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 accounts of cyber espionage originating from countries such as China, organized criminals in Russia, and the depth of the threat from Iran in the aftermath of the Stuxnet leaks originating from the current administration. Unfortunately, this bill would do little to minimize those threats or generally improve our current cybersecurity posture.

The reason for this bill's general inadequacy is that rather than using a liability protection framework to enter into cooperative relationships with the private sector, which happens to own 80 to 90 percent of the critical cyber infrastructure in this country, this bill chooses to take an adversarial approach, with government mandates and inadequate liability protections.

Further, this bill includes unnecessary items that our government cannot afford and makes no mention of what the additional programs will cost. For instance, I am sure some of us have fond childhood memories of going to or taking part in a talent show, but to include talent show provisions in this bill is ridiculous. Title IV of this bill authorizes 9th to 12th grade cyber talent shows and cyber summer programs for kindergartners to seniors in high school—again, ridiculous, especially considering that the majority leader deemed this bill more important than the National Defense Authorization Act.

While I have criticisms with every title of this bill, I will limit my comments today to title I, which regulates critical infrastructure, and title VII, which concerns information sharing among the government and the private

sector. In my view, these titles, along with weighing how much this bill, which lacks a CBO score—we do not even know how much it is going to cost—will ultimately cost and how it will dramatically increase the size of the Federal Government, are the most important aspects we can discuss.

With respect to the first title, title I, the proponents of the Cybersecurity Act would have you believe this bill authorizes the private sector to generate their own standards, that those standards are voluntary, and that the bill establishes a "public-private partnership." Unfortunately, I disagree with each of those characterizations. As the bill is currently written, the government and not the private sector would have the final say on what standards look like and the private sector would be forced to comply. While my colleagues might suggest that section 103 states that the private sector proposes "voluntary" cybersecurity practices to the government, I call your attention to the following provision in section 103, which states the government would then decide whether and how to "amend" or "add" to those cybersecurity practices. Additionally, there is no recourse for the private sector to challenge the government's actions.

Soon after the government's takeover of the development of cybersecurity standards, any notion of the standards being "voluntary" evaporates. Section 103 clearly states: "A Federal agency with responsibilities for regulating the security of critical infrastructure may adopt the cybersecurity practices as mandatory requirements." That is the language of the bill. What is being portrayed as "voluntary" proposals would soon become mandatory requirements.

Unfortunately, the conversion from voluntary to mandatory does not stop there. Shockingly, under this bill, if an agency does not adopt mandatory cybersecurity practices, it must explain why it chose not to do so. That is right. Under this bill, if a regulatory agency chooses not to mandate the "voluntary" practices, it must explain itself—as if it must be doing something contrary to the final objective. If this provision does not reveal the true regulatory intent of the proponents of this bill, nothing does.

Section 105 brings home this point by stating: "Nothing in this title shall be construed to limit the ability of a Federal agency with responsibilities for regulating the security of critical infrastructure from requiring that the cybersecurity practices developed under section 103 be met." I would very much commend my colleagues to read that provision of the bill. All you have to do is read it. The regulatory result of these standards could not be clearer.

Moving on to title VII, which deals with the flow of information between the government and the private sector, the current bill is a step in the wrong direction. Specifically, the bill would make us less safe by failing to place

the agencies with the most expertise and that are the most capable of protecting us on the same footing as other entities within the Federal Government. It strikes me as counterintuitive to prevent the institutions most capable of protecting the United States from a cyber attack and leave us reliant on agencies with far less capabilities.

Because this bill fails to equitably incentivize the voluntary sharing of information with all of the Federal Government's cyber defense assets, it does a great disservice to our national security. In cyber war, where speed and reaction times are essential to success, real-time responses are essential. The bill language states that information should be shared in "as close to real time as possible." That may sound nice, but it will not get the job done.

We all agree that the threat we face in the cyber domain is among the most significant challenges of the 21st century. It is reckless and irresponsible to rebuild the very stovepipes and information-sharing barriers that the 9/11 Commission attributed as responsible for one of our greatest intelligence failures.

Because of my opposition to this bill and the lack of a regular legislative process, I have joined with Senators CHAMBLISS, HUTCHISON, GRASSLEY, MURKOWSKI, BURR, JOHNSON of Wisconsin, and COATS in offering an alternative cybersecurity bill. The fundamental difference in our alternative approach is that we aim to enter into a truly cooperative relationship with the entire private sector through voluntary information sharing rather than an adversarial one with the threat of mandates. Our bill, which also addresses reforming how the government protects its own assets, sets penalties for cyber crimes, refocuses government research toward cybersecurity, and provides a commonsense path forward to improve our Nation's cybersecurity defenses with no new spending. We believe that by improving information sharing among the private sector and the government, updating our Criminal Code to reflect the threat cyber criminals pose, reforming the Federal Information Security Management Act, and focusing Federal investments in cybersecurity, our Nation will be better able to defend itself against cyber attacks.

Even though we do not offer talent shows or summer camps in our bill, it has the support of the industries that themselves are under attack. Before I close, I would like to leave with you a final point which gets to the heart of why we are having this debate. In our country, unlike other countries around the globe, the private sector owns 80 to 90 percent of the critical cyber infrastructure.

This is a fact in which we should all take great pride. After all, it speaks to the essence of American entrepreneurialism and our spirit of individualism. The companies that own these systems are large and small, they

employ men and women everywhere, and their influence reaches every State, every congressional district, and about every corner of our country. While we all agree we are involved in a serious national security discussion, we must not forget to weigh the economic realities of this debate too.

I caution all my colleagues to tread very carefully because I am deeply concerned we are on the cusp of granting the Federal Government broad authorities and influence over one of the most vibrant and innovative sectors of our economy. The technology sector and the use of the Internet by American companies to innovate and improve the customer experience are deeply threatened by the heavy and too often clumsy hand of government.

As we confront the security challenges of an innovative economy, we must be careful not to undermine the economy itself. It is well known that we continue to have discussions amongst various parties: Senator KYL, Senator WHITEHOUSE, Senator LIEBERMAN, Senator COLLINS. Sometimes the crowd is large, sometimes it is not so large. I think we have made some progress. I think there is a better understanding of both of the different proposals that are before us. I do believe it is important, I do believe it is very important that businesses large and small in the United States of America, whether they be the utility companies or whether they be the most high-tech sectors, be represented in these discussions. We have tried to do that.

I believe we can make progress. I believe we can reach an agreement. I also know we have had several meetings and have not had extremely measurable progress. But I am committed to doing everything I can to see we reach that agreement before we conclude the consideration of this legislation.

I would also like to point out to my colleagues that I have had numerous conversations with my friends on the other side of the Capitol. They find this legislation in its present form unacceptable. I would hope we would also consider the fact that we need to get a final bill, not just one passed by the Senate.

I yield the floor.

The PRESIDING OFFICER (Mrs. HAGAN). The Senator from Illinois.

Mr. DURBIN. Madam President, consider these ominous words:

To the loved ones of the victims who are here in this room . . . to those who are watching on television, your government failed you. Those who you entrusted with protecting you failed you. And I failed you. We tried hard, but that doesn't matter, because we failed.

Those are not my words. They contain a sentiment I hope none of us ever has to convey to the American people. Those are the words of Richard Clarke, the senior White House official who was in charge of counterterrorism efforts in the previous administration when the September 11 terrorist attacks occurred.

Mr. Clarke's testimony before the 9/11 Commission was apologetic, remorseful and tragic because he knew, he knew like no one else, our government had failed, failed to act on repeated warnings. This failure led to 9/11 and the largest loss of life on American soil at the hands of a foreign enemy since December 7, 1941, at Pearl Harbor.

Today, the national alarm security bells are ringing once again. This time, however, the enemy is not in a terrorist training camp learning how to make an explosive device or commandeer an aircraft. The enemy is not trying to sneak its way into the United States. The enemy we face does not need to hijack an airplane in order to wreck the American economy and to cause widespread loss of life. The only tool this enemy needs is a computer and access to the Internet.

The threat our Nation faces from a cyber attack will soon equal or surpass the threat from any terrorism that has consumed our attention so much since September 11. That is not my assessment. That is the assessment of the Director of the Federal Bureau of Investigation, Robert Mueller. In fact, he is not alone. There is an overwhelming bipartisan consensus among officials in the intelligence, defense, and national security community that America is incredibly vulnerable to a cyber attack that can be launched at any moment from anywhere in the world.

Michael Hayden, the former Director of the National Security Agency, Michael Chertoff, the former Secretary of Homeland Security who served under President George W. Bush, agreed. They and many other officials have joined the current Secretary of Homeland Security, Janet Napolitano, the current Director of the National Security Agency, GEN Keith Alexander, and others in warnings as follows: The cyber threat is imminent to America. It poses as serious a challenge to our national security as the introduction of nuclear weapons in the global debate 60 years ago.

The experts are sounding the alarm, telling us to take action now to prevent a catastrophic cyber attack that could cripple our Nation's economy, cause widespread loss of life, sadly send our economy into free fall. When the Cybersecurity Act of 2012 comes up for a vote, the Senate will have an opportunity to take action on this critical bill that will enhance our national security. In light of these warnings from the experts, the least we can do in the Senate is to vote to open the debate on this critically important bill.

I wish to thank its sponsors: Senator LIEBERMAN, the chairman of the subcommittee, Senator COLLINS, the ranking member, Senator FEINSTEIN of the Intelligence Committee, Senator ROCKEFELLER on the Commerce Committee. They have put a lot of time and effort into this important piece of legislation. They have worked together on a bipartisan basis. They have listened

to a wide range of comments, including a few I have offered, and I am pleased the revised Cybersecurity Act of 2012 incorporates many suggestions.

It will help make America safe by enhancing our Nation's ability to prevent, mitigate, and rapidly respond to cyber attacks. The bill contains important provisions for securing our Nation's critical infrastructure. Every day, without thinking about it, we rely on powerplants, pipelines, electric power grids, water treatment facilities, transportation systems, and financial networks to work, to live, to travel, to do so many things we take for granted.

All those critical systems are increasingly vulnerable to cyber attack from our enemies. Last year, there was a 400-percent increase in cyber attacks reported by the owners of critical infrastructure, according to the Department of Homeland Security. That increase does not even account for the many attacks that went unreported.

We do not think twice about it, but this infrastructure is the backbone of America's economy and our way of life. This bill has provisions that will help minimize our vulnerability and shore up our defenses. The bill also includes a new framework for voluntary information sharing so government agencies and private companies can improve their mutual understanding of cyber threats and vulnerabilities and develop good practices to keep us safe.

I thought it was worth doing a few months ago to call together a dozen major corporations in Chicago and across Illinois that I thought, with the advice of some people who were experts, might be vulnerable to cyber attack. I asked those experts in a closed setting, outside the press, what Congress could do to help them secure their infrastructure at their business and networks from cyber attacks.

The answer from each and every one of them was the same: We need to be able to share information on cyber threats with the government and other private entities. We need to receive information from them in order to know what they have done to effectively prevent and mitigate attacks.

Estimates are that 85 percent of America's critical infrastructure is owned by the private sector. Since we depend so much on the private sector for our critical infrastructure, the lines of communication between government and the private sector must be open. If we share best practices, the result could be to make us a secure nation.

Let me say as well, I have the highest regard for my friend and colleague Senator JOHN MCCAIN of Arizona. Senator MCCAIN's life story is a story of patriotism and commitment to America. He understands the military far better than I ever will, having served and spent so many years working on the House Armed Services Committee. But I take exception to one of his statements earlier, at least what I consider to be the message of that statement, about how we have to be extremely careful in how we engage the

private sector in keeping America safe from cyber attack.

I believe we should be open, transparent, and we should be respectful of the important resources and capacity of the private sector. But I think back 70 years now to what happened in London, when there was a blitzkrieg, and the decision was made by the British Government to appeal to every business, every home, every family, every individual to turn out the lights, because if the lights were on, those bombers from Germany knew where the targets could be found. It was a national effort to protect a nation. Should it have been a voluntary effort? Should we have had a big town meeting and said: Some of you can leave your lights on if you like, if you think it might be an inconvenience.

There comes a moment when it comes to national defense when we need to appeal to a higher level in protecting America. My experience has been that the private sector is right there. They are as anxious to protect this country as anyone. They are as anxious to protect individuals, families, even their own businesses. So this notion that somehow we are adversarial in protecting America with the private sector I do not think is the case.

In fact, Senator COLLINS is here representing the other side of the aisle. I know it is not the case. She and I have worked together. I have been very respectful of the efforts she and Senator LIEBERMAN put into rewriting the rules for our intelligence community. They did it in a thoughtful and balanced way. This bill does too.

Are there amendments we might take? Of course. This is not perfect. No product of legislation is. But I have to say I believe the private sector will be our ally, our friend, our partner in making America safe. This should not be a fight to the finish as to whether it is government or the private sector which will prevail. Ultimately, America has to prevail.

Let me say a word about one part of this bill that I played a small role in addressing. Even through the threat in cyberspace is new and emerging, it calls to the forefront a familiar attention which we witnessed in Washington; on the one hand a mutually shared goal of protecting our country, on the other hand an important obligation to safeguard constitutionally protected rights to privacy and civil liberties.

It is this tension that led us to a conversation about some provisions and trying to find the right balance. The Cybersecurity Act of 2012 is not perfect, but it effectively strikes that balance between national security and individual liberty. The bill will enhance our national security and still do it in a way that is far superior to some of the alternatives that will be offered on the floor.

CISPA, the cybersecurity act that was passed by the House of Representa-

tives, and SECURE IT, the alternative approach that has been introduced in the Senate, do not meet this standard, by my estimation. I wish to thank Senator COLLINS, Senator LIEBERMAN, and all those engaged in this conversation but special thanks to my colleague Senator FRANKEN because he is chair of the Privacy Subcommittee of our Senate Judiciary Committee.

We joined together with some colleagues: Senators COONS, BLUMENTHAL, SANDERS, and AKAKA. We asked the sponsors of the legislation to work with us and they did. The revised bill now requires that the government cybersecurity exchange, to which private companies can send threat indicators, must be operated by civilian agencies. I think that is smart.

The cybersecurity threat indicator could be a sensitive, personal communication, such as an e-mail from a spouse or private message on a social media site. As a result of our efforts, no longer can personal communications be indiscriminately sent directly to the NSA or CIA. The people who work at these agencies are fine, dedicated public servants, but these agencies are often shrouded in secrecy. I learned that as a member of the Senate Intelligence Committee.

To have the appropriate oversight, we ask that the first line of review be with a civilian agency subject to congressional oversight. This does not mean our intelligence and defense agencies will never be able to apply their experience and expertise to analyze and mitigate cyber threats. They should not be the first recipients, but the bill requires—and I think it is entirely appropriate—relevant cyber threat information can be shared by these agencies in real time. Waste no time doing it. Send it to the agencies if there is any perceived threat to America's security.

The revised bill no longer provides immunity for companies that violate the privacy rights of Americans in a knowing, intentional, or grossly negligent way—not simple negligence but things that go over that line dramatically.

I can support providing immunity for companies to share cybersecurity threats with the government, as long as they take adequate precautions and follow commonsense rules established in the bill.

The revised bill enables law enforcement entities to receive information about cyber crimes from cybersecurity exchanges without first going to court to obtain a warrant. To ensure these exchanges are not used to circumvent the Constitution and they do not create a perpetual warrantless wiretap, the bill requires law enforcement to only use information from the exchanges to stop cyber crimes, prevent imminent death or bodily harm to adults or prevent exploitation of minors.

The revised bill now requires that the rules for how the government will use

and protect the private information it receives must be in place before companies begin sending information to the new cybersecurity exchanges. That makes sense. To be sure that government agencies follow the rules for using and protecting private information, the revised bill gives individuals the authority to hold the government accountable for privacy violations.

To ensure transparency and accountability, the revised bill requires recurring, independent oversight by the inspector general and the Privacy and Civil Liberties Oversight Board.

These are commonsense reforms. Senator LIEBERMAN spoke to the Democratic Senate caucus luncheon the other day and addressed these directly. He said he took these changes to those who were in charge of our cybersecurity and said to them: Give me an honest, candid assessment. If you think this ties our hands in protecting America, tell me right now. They reviewed them carefully, debated them, and came back and said: No, these are things we can live with and work with. That is the kind of approval we are looking for from those who have this awesome responsibility.

So as a result, this bill will have my support, because I think it keeps America safe from a threat which many Americans don't even know about but could literally take or change our lives in a heartbeat. It also has the support of many progressive groups from the left and center and right. It is an indication to me we have struck the right balance.

I thank those who helped us reach this point. As with any piece of substantial legislation, there is going to be disagreement. Senator MCCAIN expressed some areas of concern. That is what debate and amendments are all about. Let's move this bill forward this afternoon. Let's entertain relevant, germane amendments. Let's take this as seriously as the threat is serious to the United States. That, to me, is the right way to go.

Again, I thank Senator COLLINS personally and all the others who made this bill a reality in bringing it to the floor for our consideration.

I yield the floor.

The PRESIDING OFFICER. The Senator from Maine.

Ms. COLLINS. Madam President, I want to rise very briefly—I know there are a number of Members who are seeking recognition—to thank my friend and colleague from Illinois for his statement today. He has worked very hard on this bill. I know it is an issue he cares deeply about, and I very much appreciate his taking the time to come to the floor and to urge Members to vote for the motion to proceed to the debate on this absolutely vital piece of legislation.

I must say I was disappointed to hear some of the comments made on the Senate floor today in opposition to this bill. The fact is both Republican and Democratic officials have, with very

JULY 26, 2012.

few exceptions, endorsed the framework of this bill and urged us to move forward. In fact, they have warned us repeatedly in saying the only question is when a major cyber attack will occur. Not whether it will occur, but when it will occur. We have letter after letter, statement after statement from national and homeland security experts, representing both President Bush's administration and the current administration, urging us to act.

Indeed, yesterday the Aspen Institute Homeland Security Group put out a statement, stating the following:

The Aspen Homeland Security Group strongly urges the U.S. Senate to vote this week to take up S. 3414, the cyber-security bill, for debate on the Floor.

The statement goes on to say:

We urge the Senate to adopt a program of voluntary cyber-security standards and strong positive incentives for critical infrastructure operators to implement those standards. The country is already being hurt by foreign cyber-intrusions, and the possibility of a devastating cyber-attack is real. Congress must act now.

This letter is signed by officials from the previous administration, such as Charles Allen, Stewart Baker, Michael Leiter, and Michael Chertoff. There are numerous representatives of past administrations and individuals who are renowned for their expertise. How can we ignore their warning that we must act, that it is urgent, and that we must have voluntary standards for critical infrastructure—infrastructure that, if it were attacked, would result in mass casualties, mass evacuations, a severe blow to our economy, or a serious degradation of our national security?

That is the definition of the core critical infrastructure we want to cover and to help make more secure through a partnership with the private sector. And it has to be a partnership because 85 percent of critical infrastructure is owned by the private sector. We have worked hard to alter our bill to take suggestions from the private sector, from our colleagues, from the administration, and from experts across the philosophical range to improve our bill.

I heard a Member saying this morning that somehow we are going to be hurting the high-tech sector of our society. Well, that is not what Cisco and Oracle think—certainly two of the leading businesses in the high-tech sector. This morning they wrote to us, the chief sponsors of the bill—Chairman LIEBERMAN, Chairman ROCKEFELLER, Chairman FEINSTEIN, myself, and Senator CARPER—and I want to read a brief excerpt from their letter. They said:

... we appreciate your efforts to craft legislation that addresses the important issue of cybersecurity by supporting American industry in its efforts to continue to be the world's leading innovators.

The fact is, it is American businesses that are being robbed of billions of dollars every year due to cyber intrusions from foreign governments, from transnational criminals, and from hackers. This is a threat not only to

our national security but to our economic prosperity.

That is why the letter from Cisco and Oracle goes on to say:

We praise your continued recognition of the importance of these objectives through the provisions of S. 3414.

They say they support those provisions. Continuing to read from the letter:

We also commend your commitment to ensuring that the IT industry maintains the ability to drive innovation and security into technologies and the network.

So the idea we heard this morning on the Senate floor that somehow we are going to bring innovation in America to a standstill or hurt this important sector of our economy is not supported by a reading of our bill, and it is certainly contradicted by the letter we received from Cisco and Oracle, leading companies in the high-tech sector.

Finally, I would point out they thank us for our outreach, our willingness to engage in an exhaustive process around this issue set, and to consider and to respond to the views of America's technology sector. That is what we have done. That is what we are continuing to do with our colleagues on both sides of the aisle who bring varying views to this issue. But what we cannot do is to fail to act when the warnings are so constant and alarming about the threats to our Nation, to our economy, and to our way of life.

Madam President, I ask unanimous consent to have printed in the RECORD the statement from the Aspen Institute Homeland Security Group as well as the July 26 letter from Cisco and Oracle.

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

JULY 24, 2012.

STATEMENT OF THE ASPEN HOMELAND SECURITY GROUP

The Aspen Homeland Security Group strongly urges the U.S. Senate to vote this week to take up S. 3414, the cyber-security bill, for debate on the floor. We urge the Senate to adopt a program of voluntary cyber-security standards and strong positive incentives for critical infrastructure operators to implement those standards. The country is already being hurt by foreign cyber-intrusions, and the possibility of a devastating cyber-attack is real. Congress must act now.

Charles E. Allen; Stewart A. Baker; Richard Ben-Veniste; Peter Bergen; Michael Chertoff; P.J. Crowley; Clark K. Ervin; Jane Harman; Michael V. Hayden; Michael Leiter; James M. Loy; Paul McHale; John McLaughlin; Philip Mudd; Eric T. Olson; Guy Swan, III; Juan Zarate; Philip Zelikow.

Hon. JOSEPH I. LIEBERMAN, Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

Hon. SUSAN M. COLLINS, Ranking Member, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

Hon. JOHN D. ROCKEFELLER, Chairman, Committee on Commerce, Science and Transportation, U.S. Senate, Washington, DC.

Hon. DIANNE FEINSTEIN, Chairman, Select Committee on Intelligence, U.S. Senate, Washington, DC.

Hon. THOMAS R. CARPER, U.S. Senator, Washington, DC.

DEAR SENATORS LIEBERMAN, COLLINS, ROCKEFELLER, FEINSTEIN and CARPER: As two of the industry-leading companies providing information technology across the nation and the world, we appreciate your efforts to craft legislation that addresses the important issue of cybersecurity by supporting American industry in its efforts to continue to be the world's leading innovators. This matter deserves the continuing attention of industry, the Congress and the Administration, and we commend you for having constructively engaged stakeholders throughout this process.

As you know, effective cybersecurity must be driven by an IT industry that is free to drive innovation and security and maintain world leadership in the creation of secure systems. Effective cybersecurity depends on our having the ability to drive innovation globally—it is our core value. We have long advocated a cybersecurity approach based on the importance of real information sharing that can help protect important assets. We thank you for your leadership in recognizing that any cybersecurity legislation must incorporate iron-clad protections to ensure American industry remains the world's leader in the creation and production of information technology, and to make certain that legislation maintains and protects industry's ability and opportunity to drive innovation and security in technologies across global networks.

We praise your continued recognition of the importance of these objectives through the provisions of S. 3414, the Cybersecurity Act of 2012. The provisions regarding the designation of critical cyber infrastructure, the specifics of cybersecurity practices, and the treatment of the security of the supply chain demonstrate your continued recognition of these core principles, and we support them. Wherever the important cyber debate takes this legislation, these core principles should be promoted and preserved. We believe these provisions as written capture that principle and believe it is in the interest of cybersecurity and critical infrastructure that they remain explicit. We also commend your commitment to ensuring that the IT industry maintains the ability to drive innovation and security into technologies and the network. Further, we appreciate the recognition that more needs to be done in advancing innovation through increased research and development, and in raising awareness and education, and importantly on increasing global law enforcement.

By explicitly maintaining these principles and provisions, your legislation proposes a number of tools that will enhance the nation's cybersecurity, without interfering with the innovation and development processes of the American IT industry. Ultimately, the ability of the tech industry to continue to innovate will provide the best defense against cyber attacks and data breaches.

We also note the shift toward a voluntary framework for critical cyber infrastructure in the new bill, and commend and support the great strides you have made toward that goal. We look forward to continuing to work with you on this issue.

We thank you for your outreach, willingness to engage in an exhaustive process around this issue set, and to consider and respond to the views of America's technology sector. We look forward to working with you and others in the Congress to continue the public-private collaboration and to make sure that what results continues to meet our common goals.

Sincerely,

BLAIR CHRISTIE,
Senior Vice President and Chief
Marketing Officer, Government Affairs,
Cisco Systems, Inc.
KENNETH GLUECK,
Senior Vice President, Office of the CEO
Oracle Corporation.

Ms. COLLINS. Madam President, I yield the floor.

The PRESIDING OFFICER. The Senator from Minnesota.

Mr. FRANKEN. Madam President, I rise today to talk about our Nation's defenses against cyber attacks, and I wish to commend the Senator from Maine for her leadership. She is the ranking member, of course, on the Committee on Homeland Security and Governmental Affairs. I wish also to commend all three chairs, Senators LIEBERMAN, FEINSTEIN, and ROCKEFELLER, for their work.

As I said, I rise today to talk about our Nation's defense against cyber attacks and how our Nation needs to respond to those threats which affect our national security, our economic security, and our privacy.

News reports and experts confirm our Nation's critical infrastructure, such as our water systems, our power grid and so forth, are vulnerable to attacks from hackers and foreign governments. Every few weeks we hear about yet another breach—Yahoo and Gmail, Citibank, Bank of America, Sony PlayStation. Millions of people have had their names, passwords, credit card information or health information compromised.

It isn't just our national security or economic well-being that is being threatened by these attacks, it is the Internet itself. If you want to use Facebook or a cloud-based e-mail provider to communicate with your friends and loved ones, you need to know that your private communications won't be exposed by hackers. If you want to use the Internet to spread new ideas or fight for democracy, you need to know your work won't be disrupted by hackers or repressive regimes.

Unfortunately, it is hard to write a good cybersecurity bill, because when you try to make it easier for the government or Internet companies to detect and stop the work of hackers or other bad actors, you often end up making it easier—or very easy—for those same entities to snoop in on the lives of innocent Americans.

Until recently, every major cybersecurity bill on the table would have

done too much to immunize and expand the authority of the government and industry and far too little to protect our privacy and civil liberties. These bills would make it too easy for companies to hand over your e-mails and other private information to the government—even to the military. Setting aside the fourth amendment, these bills would allow almost all of that information to go to law enforcement. And these bills do far too little to hold these companies and the government accountable for their mistakes.

A few months ago, I teamed up with Senators DURBIN, WYDEN, SANDERS, COONS, BLUMENTHAL, and AKAKA to try to address this situation. We worked with privacy and civil liberties groups on the left, the right, and the center to come up with a package of proposals. We worked with the ACLU, the Electronic Frontier Foundation, and the Center for Democracy and Technology, which are traditionally associated with progressives; we worked with the Constitution Project, which is a bipartisan centrist think tank; and we worked with TechFreedom and the Competitive Enterprise Institute, which are conservative libertarian organizations.

Together, we approached Chairman LIEBERMAN, Ranking Member COLLINS, Chairman ROCKEFELLER, and Chairman FEINSTEIN, and proposed a package of amendments to the information-sharing title of the Cybersecurity Act of 2012.

The information-sharing title is the part of the bill that will make it easier for companies to share critical information about cyber attacks with each other and with the government. These Senators engaged with us earnestly and in good faith. After a lot of hard work and a lot of conversations, the sponsors made a series of changes to the bill that are major, unequivocal victories for privacy and civil liberties.

The bill is still not perfect, from my point of view, but I can say with confidence that when it comes to protecting both our cybersecurity and our civil liberties, the Cybersecurity Act of 2012 is the only game in town.

I want to take a moment to explain the changes made to the information-sharing title, and compare how the Cybersecurity Act now stacks up with its rival bills, the Cyber Intelligence Sharing and Protection Act, or CISPA, which recently passed the House, and the SECURE IT Act, which has been introduced here in the Senate.

First of all, I agree we need to make it easier for companies to share time-sensitive information with experts in the government. But the cyber threat information that companies are sharing often comes from private, sensitive communications, like our e-mails. And so the gatekeeper of any information shared under these proposals should never be the military. It should never be the NSA. The men and women of the NSA are patriots and they are undoubtedly skilled and knowledgeable. But as Senator DURBIN said, that institution

is too shrouded in secrecy. And—he didn't say but as I will say—it has too dark a history of spying on innocent Americans to be trusted with this responsibility under any administration.

Under the new, revised Cybersecurity Act of 2012, the one that will soon be before us on the floor, companies can use the authorities in the bill to give cyber threat information only to civilian agencies. That is a critical protection for civil liberties, and it is a protection that CISPA and the SECURE IT Act do not have. I want to be very clear. An America with CISPA and an America with the SECURE IT Act is an America where your e-mails can be shared directly, immediately, and with impunity, with the NSA.

Second, any cybersecurity bill should focus on just that—cybersecurity. It should not be a back door for warrantless wiretaps or information entirely unrelated to cyber attacks. In other words, once a company gives the government cyber threat information, the government shouldn't be able to say, Hey, this e-mail doesn't have a virus, but it does say that Michael is late on his taxes; I am going to send that to the IRS.

Under the Cybersecurity Act of 2012, once a cyber exchange gets information, it can give that information to law enforcement only to prosecute or stop a cyber crime or to stop serious imminent harm to adults or serious harm to minors. CISPA actually has similar protections, but SECURE IT allows a far broader range of disclosures to law enforcement. Here in the Senate, the Cybersecurity Act is the proposal that does the most to respect the spirit and letter of the fourth amendment.

Third, a cybersecurity bill should make it easier for a company to share information with experts in the government. But it has to hold companies that abuse that authority accountable for their actions. Both CISPA and the SECURE IT Act give companies immunity for knowing violations of your privacy. Under CISPA and the SECURE IT Act, if a company's CEO knows for a fact that his engineers are sending every one of your e-mails to the NSA, there is nothing you can do about it. That is not an exaggeration. Thanks to the changes I have pushed for—along with Senators DURBIN, WYDEN, COONS, SANDERS, BLUMENTHAL, and AKAKA—the Cybersecurity Act does not protect companies that violate your privacy intentionally, knowingly, or with gross negligence.

Fourth, and finally, a cybersecurity bill should also hold the government accountable for its actions. Under both CISPA and the SECURE IT Act, companies can start giving the Federal Government your private information well before the government actually has privacy rules in place for how to handle that information.

Under the SECURE IT Act, the government has total immunity from lawsuits arising out of its cybersecurity

operations—total immunity for the government. The SECURE IT Act also lacks any regular independent oversight of the Federal Government's actions under these new authorities. The Cybersecurity Act of 2012 now has all three of these protections. Under this bill, privacy rules have to be in place on the first day companies start giving the government information. People can sue the government when it abuses its authority. And there will be recurrent, independent oversight by both the Privacy and Civil Liberties Oversight Board and inspectors general.

These are just the four main categories of changes that the sponsors of the Cybersecurity Act have adopted. There are other changes, too, that I won't go into now.

Before I close, I want to elaborate on one way I do think we need to improve the Cybersecurity Act to better protect privacy. The sponsors of the bill have rightly adopted several critical protections. I hope they will accept at least one more amendment that I think is very important. I will talk about my amendment more on another occasion, but for now I want to flag it for my colleagues.

For decades, Federal law has given Internet service providers and other companies the right to monitor their systems to protect themselves and their customers from cybersecurity threats. They also have the right to deploy what are called countermeasures to protect their systems against those threats. So these companies have the right to monitor and protect themselves; but at the same time, Federal law prevents them from abusing those rights. If an ISP starts randomly picking customers and reading their e-mails, their customers—and the government—can take them to court, and the ISP can't throw its hands up and plead cybersecurity.

This is why, when the President of the United States brought together all of the Federal agencies to craft a bill that would comprehensively protect our cybersecurity, that proposal included a new authority for companies to disclose information to the government but contained no new authority for companies to monitor e-mail or deploy countermeasures. When the administration's lawyers were asked why that was, they said that doing so would have been duplicative—duplicative—because the companies already have those rights.

Right now, the Cybersecurity Act and the President's proposal are not in line with each other, because unlike the President's proposal, the Cybersecurity Act does give ISPs and other companies a brandnew right to monitor communications and to deploy countermeasures. That right is very broad—so broad that if a company uses that power negligently to snoop in on your e-mail or damage your computer, they will be immune from any lawsuit. I plan to offer an amendment to delete these new monitoring and counter-

measures authorities and bring this bill in line with the President's proposal. I hope my colleagues here in the Senate will join me in passing this amendment. Seven of my colleagues have already indicated they will co-sponsor this amendment.

But I want to end on a high note. I don't want my amendment to cloud my central message here, so I will repeat what I said earlier. The Cybersecurity Act is not perfect, but when it comes to striking a balance between cybersecurity and privacy and civil liberties, it is the only game in town. It is far more protective of our rights than either CISA or the SECURE IT Act. I thank the sponsors of the Cybersecurity Act for taking this high road, and I urge my colleagues to vote to proceed to the bill so we can have a good, full debate on it.

Madam President, I yield the floor.

The PRESIDING OFFICER. The Senator from Delaware.

Mr. COONS. Madam President, I am honored to be able to join the Senator from Minnesota in speaking today in support of all the Members of this body voting to proceed to the consideration of the important cybersecurity bill to which he and Senator DURBIN have spoken.

Today we have an opportunity to celebrate progress—very real, very concrete, and very important progress—in the legislative efforts to make America both more secure and yet retain our core constitutional freedoms: the protections of privacy that Americans have held dear from the very beginning of this Republic.

As I have said before on this floor, taking action to protect our Nation from the very real and urgent threat of cyber attack is of paramount importance, something so urgent that it deserves our undivided attention. But so is protecting the privacy rights of law-abiding American citizens.

As we work together toward this commonsense, compromise piece of legislation the Senate should consider in coming days, I fought hard, along with several colleagues, to ensure we maintain the right balance between privacy and security. That balance is essential. Compromising our liberty would be as dangerous as compromising our safety. But thanks to the hard work of so many of my colleagues—in particular Senator DURBIN, Senator FRANKEN, Senator BLUMENTHAL, Senator MERKLEY, Senator SANDERS, and others—we found that appropriate balance in this legislation that is before us.

The changes we have made to the original text and to the House-passed version have significantly strengthened privacy rights. That is why I say we can celebrate real progress here today.

I long thought it was the privacy issues that would be the rock on which this ship would founder, that the critical and unaddressed privacy issues in CISA and SECURE IT, spoken to by Senator FRANKEN, would be issues that would prevent me from supporting cy-

bersecurity legislation in this session of Congress. But we have made remarkable progress. Let me briefly review a few of the areas where that progress has been made.

We made sure companies cannot pry into the private online activities of everyday Americans in the name of national security. I want to mention one more improvement.

In addition to those mentioned by Senator FRANKEN just before me concerning legal immunities contained in this bill, this bill appropriately gives companies the authority to share cyber threat-related information with each other and the government, without which we can't know what the rapidly emerging significant national cyber threats are. It also gives them immunity from suit if they do so. So if companies share with each other real-time cyber threat information, they cannot be sued. But prior versions of this bill might have provided bad actors with immunity against all privacy laws. So instead, we added tough provisions to ensure if a company acts recklessly or willfully to violate the law and the online privacy of its customers, they will be held accountable. This legislation now, in my view, strikes an appropriate balance between empowering companies and providing them certainty, as well as maintaining the privacy rights of Americans and their customers.

In this new, better, stronger legislation, it is no longer the case that companies can share your data and violate your privacy because you interact with them online. If that had remained in this bill, I would have expected millions of Americans to mobilize to stop this legislation. But we are here today as a group of Senators to announce that real progress has been made, and we are comfortable with and support this legislation from a privacy perspective.

I urge my colleagues, when we take up this vote later this afternoon, to vote to proceed to the bill and to allow us a full and robust debate on this cybersecurity legislation.

Getting to this new and improved legislation was a team effort, and special credit is due to Senators LIEBERMAN and COLLINS for leading the way, for being willing to find common ground on challenging issues. There was also a great deal of work done by my senior Senator TOM CARPER and by Senators FEINSTEIN and ROCKEFELLER who chair committees and were also essential to making such great progress.

One of the aspects of cybersecurity and the threat to our country that keeps me up at night is that it is constantly evolving. Our enemies are smart, they are capable, and they are fast. That means our cyber defenses have to be flexible, adaptable, and regularly evaluated in order to keep up.

One good thing about the House version of this legislation is that it includes a sunset provision requiring that in 5 years, this body once again

must take a hard and serious look at cybersecurity threats, and update or change our defense as needed, and ensure that privacy protections have been fully observed.

That is not just good strategy, it is good sense. Think about the capabilities of your computer, your cell phone 5 years ago compared to today. The pace of change is faster online than ever before, and we need the kind of legislative process that allows us to review our work and ensure not only that we stay ahead of the curve in defending our country but we continue to strike the right balance between privacy and security.

That is why, similar to Senator FRANKEN before me, I intend to introduce an amendment on the floor—which I hope will earn consideration by this body and the support of my colleagues—to take the sunset provision of our House counterparts and match that in the Senate in this bill. It is the right thing to do to help keep us safe and to help our military leaders and cybersecurity experts stay one step ahead of those who would wish us harm.

In closing, I thank Senator WHITEHOUSE, who has been an important part of two different teams working on this bill. Senators KYL and WHITEHOUSE led a team that worked hard on critical infrastructure. I wish to thank Senator BLUMENTHAL of Connecticut, who participated in the privacy side work and in the critical infrastructure work. Now we are speaking to title VII, to the information-sharing provision of the bill and the dramatic and real progress that has been made in addressing the balance between security and privacy.

There has also been great progress made, in my view, in addressing the issues of critical infrastructure, and I invite Senator BLUMENTHAL of Connecticut, who has contributed so well to both these efforts, to address the Chamber at this time.

I yield the floor.

The PRESIDING OFFICER (Mrs. McCASKILL). The Senator from Connecticut.

Mr. BLUMENTHAL. Madam President, I thank my very distinguished and effective colleague from Delaware for his great work as part of a team that has sought to enhance the protections of privacy in this bill. His perspective as a local official, as a constitutional expert, as someone who cares deeply about privacy and civil liberties, has been invaluable to this effort. He too has participated in the critical infrastructure team which both of us have been privileged to join with Senators WHITEHOUSE and KYL, who have been so enormously helpful in this effort. I join him as well in thanking our colleagues Senators AKAKA, DURBIN, FRANKEN, SANDERS, and WYDEN for their very important efforts to protect privacy and civil liberties in the information-sharing title of the cybersecurity act.

We have truly worked as a team and, in many ways, a bipartisan team in forging this legislation. Of course, we have followed the lead of Senators LIBERMAN and COLLINS who have been at the forefront of this effort, as well as Senators ROCKEFELLER, FEINSTEIN, and CARPER, who deserve our appreciation for drafting the bill, shepherding it through committee, and bringing a modified version to the floor where now we have the historic opportunity to move forward. I am here to urge my colleagues, in fact, to move forward and vote to proceed to the bill later today.

We have made good progress on this legislation. I am optimistic that we will pass a cybersecurity bill in the very near future—as we must for all the reasons that have been articulated by myself and others. This Nation is under attack. It is under cyber attack. Literally, every day our defense industrial base, our military systems, and our private industry are under attack by nations and by hackers, both sophisticated and unsophisticated, abroad and at home. We must make sure we provide the tools and the resources, legal resources and authority to stop that attack, to deter it, to defeat it, to make sure our country is defended against it effectively and comprehensively.

The nature of defending against cyber attack involves information sharing. There is no way around that basic fact that information about the attacks—the sources, the objects and targets, the times—all the details are, in essence, the power to defend. Information is power when it comes to defending against cyber attack. Yet we also know that information, when shared, can also be abused. Some of the most tragic chapters of our Nation's history have involved snooping, spying, surveilling, and then sharing of information that is inappropriate and unnecessary and sometimes illegal.

We know also that one of our core constitutional protections is, in fact, the right to privacy. It is enshrined in our Constitution. It dates from our founding. It is integral to the fabric of the rule of law. We resisted and rejected the rule of the British, in part, because they had no respect for the privacy of the colonials. That basic value has inspired the rule of law since.

There is a saying—I believe it is a Latin saying—that in war, law is the first casualty. We are in a cyber war, but our constitutional law cannot be a casualty. Our right to privacy and civil liberties must be protected.

Information sharing must involve the right information shared with the right people and officials for the right purposes. There must be red lines and red lights. There must be consequences if those red lines or red lights are disregarded or dismissed.

This bill meets those basic requirements. It is enforceable and it must be enforced. In fact, I will offer an amendment to increase the enforceability and

enforcement of these basic protections by increasing the penalties for violating these basic protections. The trust and confidence of our Nation in the rule of law depends on our getting it right: information sharing with the right information to the right people and for the right purposes.

The kinds of modifications contained in this bill are critically important. They are in sharp contrast to the House-approved version of CISPA, which utterly fails to protect civil liberties and privacy rights in sufficient degree. Unlike past versions, this measure establishes unequivocal civilian control of cybersecurity information exchanges. Unlike past versions, this bill bars companies from using cybersecurity as a pretext for violating FCC net neutrality rules. Unlike other versions, this bill bars companies from using cybersecurity as a pretext for violating other guarantees, and it allows citizens to hold companies accountable and take them to court for knowingly or grossly negligent violations of the information-sharing provisions of this bill.

Equally important, it enables them to hold the U.S. Government and other public officials responsible and take them to court if they violate the privacy guarantees in this bill.

A private company receiving someone's private information while monitoring for cyber threat should protect that information. It is a public trust and a public responsibility. This act protects Americans' privacy by requiring companies that obtain that kind of information—some of it medical or financial of the most confidential and private nature—through monitoring, to protect that information.

This measure also imposes restrictions on the use of shared information for law enforcement purposes. The government can only provide information to law enforcement if it relates to a cyber crime or a serious threat to public safety; that is, physical safety—bodily harm. Law enforcement can only use information to prosecute or stop cyber attacks to prevent that kind of imminent and immediate harm to a person or a child.

There are other protections—some of them have been mentioned by Senators FRANKEN and COONS before me—that I will support. For example, Senator FRANKEN mentioned that his amendment would eliminate new authorities in the bill to monitor communications or operate countermeasures. Senator COONS mentioned a 5-year sunset on the use of information sharing under this measure to help guard against unforeseen consequences of the legislation and ensure that congressional oversight occurs on a regular and foreseeable basis. Other measures which I consider important would require Federal agencies that suffer a data breach to notify affected individuals and allow those individuals to recover damages and require the creation of a new office in the Office of Management and Budget, that of Chief Privacy Officer.

I support these amendments and I support also increasing the penalties in the event that government or companies violate the protections in this statute.

We have indeed made progress. There is more to do. I hope more progress will be made. I foresee passage of a cybersecurity measure that is desperately and direly needed in this country—not at some point in the future but now. As others before me have said on this floor and as I have said before, cybersecurity is national security and we must protect our national security while at the same time retaining the reason, our fundamental rights and civil liberties, that we want to protect our Nation and its constitutional values.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The assistant legislative clerk proceeded to call the roll.

Mr. MORAN. Madame President, I ask that the order for the quorum call be rescinded and that I may speak as in morning business.

The PRESIDING OFFICER. Without objection, it is so ordered. The Senator may speak as in morning business.

MEATLESS MONDAY

Mr. MORAN. Madam President, yesterday I was on the Senate floor, and I had the opportunity to highlight a development at the Department of Agriculture. We learned yesterday afternoon that the Department of Agriculture, in an employee newsletter, was promoting something called Meatless Mondays. The Department of Agriculture newsletter offered encouragement for its employees and I assume others who might see the newsletter—even tourists who visit Washington, DC, and eat at the Department of Agriculture cafeteria—to participate in Meatless Monday. It indicates the desirability of reducing the consumption of meat and dairy products. I found that very startling and surprising. Never in my life would I expect the Department of Agriculture, which I always presumed is the farmers' and ranchers' friend, to be promoting the idea that it is a bad idea to eat the products of farms and ranches across Kansas and our Nation. Yet that is what we saw and read yesterday.

The Department of Agriculture newsletter said that "beef production requires a lot of water, fertilizer, fossil fuels, and pesticides. In addition, there are many health concerns related to excessive consumption of meat." Those are the words of the Department of Agriculture newsletter. I am pleased to report that in asking Secretary Vilsack to reconsider what the Department had said and was promoting, they have done that and they have apparently removed the promotion from their newsletter and from their Web site. That is a positive development, and so I appreciate that happening.

It is amazing to me, unfortunately, that this is just one of many cir-

cumstances in which we see administration agencies and departments on the side of something that those of us who believe strongly in traditional family agriculture across the country believe is very important. One would expect in this case that the Department of Agriculture would promote the consumption of meat. In fact, within the Department of Agriculture, we have the Secretary saying in his mission statement that he is about increasing and expanding domestic and foreign markets for beef and meat products. We have the U.S. beef board, organized and monitored by the Department of Agriculture, whose job it is to promote agricultural products. Many of us in Congress try to encourage the sale of agricultural products, particularly meat and beef products, to South Korea and China. We have debated on the Senate floor the value of trade agreements, most recently with Colombia, South Korea, and Panama, because we believe in the opportunity for American producers to sell their products around the globe. Yet we saw at least some at USDA who have the view that we need to discourage the consumption of meat for environmental and health reasons.

Particularly troublesome is the fact that the Department of Agriculture was citing the United Nations as a reason that we ought to discourage the consumption of beef for environmental reasons. Our Department of Agriculture positions ought to be based upon sound science, not some U.N. study.

Beef is an important and vital component of the Kansas economy. We are the second largest beef-producing State in the country. The economic impact to our country is around \$44 billion. Beef exports in 2011 were over \$4.08 billion. This matters to us greatly.

This is happening at a time in which to the cattle producers across the Midwest, including in the State of the President today, the drought is so damaging.

It is also happening at a time in which we have been having the debate about the farm bill. My farmers in Kansas will often say: I know we need to do something about reducing spending. We have to get the deficit under control.

In fact, the farm bill we passed in the Senate has a reduction in the farm bill spending of \$23 billion. No one likes to see something that is important to them go away, but if this farm bill becomes legislation and direct payments leave, the safety net for producers across our country will be less. Yet farmers and ranchers say: We have a responsibility as American citizens to give these things up, to reduce the spending that comes our way, but please don't do anything that is damaging to us as far as our ability to earn a living in the free market, in the real world.

So when we see something like this from the Department of Agriculture

discouraging the use of meat products—and, again, at a time in which the temperatures across my State have been over 100 degrees for more than a month. We had a record high of 118 degrees. Perhaps that is a record high on the globe. It certainly is in the United States. In Norton, KS, it was 118 degrees. Rain is so scarce, we spend a lot of time in our State down on our knees praying for moisture and we spend a lot of time looking up to the skies hoping for moisture. We need to make sure that what we do in this Congress and what the Obama administration does is not something that diminishes the chances for the survival of family farms in the United States, certainly at home in Kansas and around rural America.

If this was just an isolated instance, perhaps the point has been made and the words have been withdrawn, but I remember we started a year ago with a Department of Labor that concluded that we need to regulate the use of 14- and 15-year-olds on family farms. That was a real misunderstanding of how production agriculture and family farms work. Agriculture is a family operation, and yet we had the Department of Labor suggesting that someone 15 years old should perhaps not be able to work on their own family's farm. I remember just 6 months or so ago, I was on the Senate floor worried about a Department of Agriculture forum on animal safety that was being organized by the Humane Society. Again, my farmers and ranchers would say—particularly in a time of drought and where the safety net provided by the farm bill is going to become less—please don't do anything that is harmful to us, that reduces the chance for us to succeed.

In this regulatory environment in which we find ourselves, we need to take the steps that promote agriculture, not do things that diminish the opportunity for a farmer or rancher to earn a living in the free market.

Yesterday we had a debate about estate taxes and the consequences to family agriculture across the country, and again, at a time in which the drought is so prevalent, circumstances so difficult, the Tax Code matters greatly and the ability to pass a family farm from one generation to the next is critical. It is so much about agriculture in States such as mine that when our farmers and ranchers don't succeed, the success of the communities in which they live and raise their kids greatly diminishes. This is a way of life for us, and we need to make certain we have a Department of Agriculture that is promoting our farmers and ranchers and their success.

I was on the Senate floor yesterday with the Senator from Wyoming. We had a conversation about the drought, the estate taxes, and the farm bill. I am interested if the Senator from Wyoming has any further thoughts. I know he is a leader in the Western Caucus. As Members of the Senate, we are in

the process of writing Secretary Vilsack in regard to the promotion of Meatless Monday. There are those who have a different view about what their menus should be and what they want to see on the menu, and that is fine with me. That is a personal decision. But the Department of Agriculture ought to be supportive of the people who produce the food, fiber, and energy for our country each and every day. They get up at sunrise and go to bed after sunset because they are out there trying to make a living on family farms across the country.

I yield for the Senator from Wyoming.

Mr. BARRASSO. Madam President, never in my life would I expect to see the U.S. Department of Agriculture come out against farming, ranching, agriculture, and its products.

I was talking to a radio station this morning in Afton, WY. They were astonished. They had not heard the news of this yet, and they are now fully aware of it. They are grateful to the Senator from Kansas because one of those involved actually had heard the Senator on the floor last night talking about Meatless Mondays and then the USDA linking ranching and farming to climate change. It is not just cattle or beef producers—and beef is clearly the No. 1 cash crop for Wyoming—but the USDA has gone after dairy products, such as milk and cheese, as part of a climate change issue.

So this does seem to be an assault against a way of life, a significant part of our country's heritage, as well as our economic future. We see this assault on our products through the Department of Agriculture. We see it as an assault on family values of young families working together, as we have seen with the Department of Labor. And now yesterday, with a vote on this Senate floor, there was an attack by a reinstitution of the death tax. People are trying to keep a family operation within the family, a ranch or a farm, all across rural America. These small businesses in communities all across the country are finding that it is going to be much more difficult, under what the Democrats voted for yesterday, to keep their ranches and farms in the family.

I know farmers and ranchers in Wyoming where a member of the family works in town just to make the money to pay the expenses of keeping the operation of the farm or the ranch going. They know full well that under the Democratic proposal, if someone were to die, once that becomes the case, their chances of being able to hold on to that operation are reduced to almost nothing. Bringing back the costs of the death tax to the levels of the Clinton administration, anything over \$1 million in assessed value would be taxed at 55 percent. The only solution for many is to sell.

There are three specific attacks: the death tax attack, the Meatless Monday attack, and the attack on children

helping out on the family or neighbor farm or ranch. There are values that they learn through the FFA. All of those things make me wonder in what direction the country is heading. I guess that is no surprise when only one in three Americans all across the country think the country is heading in the right direction.

I am happy to join my colleague from Kansas who came to the Senate floor yesterday to bring this to the attention of the Senate. He and I are working together to now address the Secretary of Agriculture to make sure that something like this doesn't happen again and to make sure that the Secretary does insist that farmers and ranchers across this country—and the products that they make and should be promoted by the Department of Agriculture—receive the proper honor that is deserved by them for what they do to continue to put food on the table and continue to bring forth the values from those who built this great country.

I thank my friend and colleague, the Senator from Kansas, for bringing this to the attention of the Nation.

Mr. MORAN. Madam President, just to conclude my remarks, I would indicate that my family and I will be eating more beef, not less. I would urge Americans to respond in that way. It is an opportunity for us to support the cattlemen and the livestock producers of our country at a time when they are selling their herds because the drought is so severe that there is no grass and no feed to feed the cattle. As a result, the market is depressed and prices are lower because there are so many sales occurring. We can help our livestock producers, our farm and ranch families in the country, by having a hamburger or steak. Let's go back to that traditional American meal of "let's eat beef." The front of my truck at home says "Eat Beef," and I would encourage Kansans and Americans to do so at this time when our livestock producers, due to the drought, are struggling so greatly.

I yield the floor.

The PRESIDING OFFICER. The Senator from Wyoming.

Mr. BARRASSO. I ask unanimous consent to speak as in morning business.

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

A SECOND OPINION

Mr. BARRASSO. Madam President, I come to the floor today, as I do week after week since the health care law was passed, to give a doctor's second opinion about the health care law that I believe is bad for patients, bad for the providers, the nurses and the doctors who take care of those patients, and terrible for the American taxpayers.

I come to the floor today reminding myself and the Senate of some promises the President made during the health care debate. The President had a couple of key promises. The first was he stated that health insurance premiums would go down. The second

promise he made was that if a person likes their insurance plan, they can keep it.

The President actually reiterated the second point after the Supreme Court issued its decision regarding the health care law a few weeks ago. From the East Room of the White House, the President proclaimed:

If you're one of the 250 million Americans who already have health insurance, you will keep your health insurance.

Perhaps the President does not know that his health care law has already forced many colleges and universities to stop offering their student health plans or perhaps the President is unaware that one can no longer purchase a child-only health insurance policy in many States, including my home State of Wyoming.

Apparently, the President has not spoken to businesses across the country that must actually deal with the ramifications of his health care law. I speak with business owners around Wyoming every weekend as I travel around the State, and the people with whom I speak believe the law will increase the cost of their insurance, increase the cost of their care, and make it more difficult for them to provide insurance for their employees.

Now we have a new study—a report that has come out from the Deloitte consulting firm—and it has spoken to businesses all across the country about the law. The results were compiled in their 2012 survey of employers. In this report, the company did random surveys of 560 companies with 50 or more employees. These results are only from companies that currently offer health insurance to their employees.

So what are the results? Well, the results are not encouraging. They found that approximately 1 in 10 employers is considering dropping the health coverage they currently supply to their employees over the next few years. Specifically, they found that 9 percent of companies expect to drop their insurance coverage, while another 10 percent of respondents said they weren't sure about how they would proceed. The survey revealed that small businesses—those with between 50 and 100 workers—are going to be hit especially hard by this new health care law.

Thirteen percent of the businesses in this category stated they would drop their insurance coverage in the next 1 to 3 years. Thirteen percent of all of those small businesses with between 50 and 100 employees plan to drop their insurance within 1 to 3 years.

Keep in mind that the nonpartisan Congressional Budget Office did some evaluations and thought that only 7 percent of workers would lose their employer-provided health insurance starting in 2014 because the President, looking straight into the camera straight from the White House, said, "If you like what you have, you can keep it."

Companies also made it clear that how implementation of the health care law moves forward would impact their

decisions. How so? Here is an example: Approximately one-third of the companies stated they might decide to stop offering health insurance if they find that the law passed by the Democrats in this Senate, along partisan lines—if these companies find that the health insurance under the law and required by the law requires them to offer more generous benefits than they currently provide, they are likely—one-third—to discontinue providing health insurance.

Why is that? Well, it is because the President's health care law actually mandates what kind of insurance companies must give to their employees. This is what is called the essential health benefits package or, as most Americans refer to it, government-approved insurance. It may not be the insurance you want or the insurance you like; it may not be the insurance you need or it may not be the insurance you can afford. No matter how we look at it, the President and those who supported this law say they know better than American consumers, American workers, and people in need of insurance.

So instead of allowing businesses and workers to decide what kind of insurance they need, the health care law empowers Federal bureaucrats to make this decision.

In an article that recently appeared in the *Wall Street Journal*, the chief financial officer of McDonald's stated that he thought implementing the health care law could cost his company more than \$400 million a year. So businesses that decide they can't afford to offer this government-approved insurance are going to be forced to pay a penalty.

How big is the penalty? That is a legitimate question. The Supreme Court says it is a tax—a tax. So they are going to have to pay a tax. So for companies with over 50 employees, they will have to pay, starting at \$2,000 per worker. That sounds like a lot of money, but keep this in mind: In 2011 the Kaiser Family Foundation found that the average cost of employer-provided health insurance for families was over \$15,000. So they can decide: Do they pay the government \$2,000, that tax, or do they pay \$15,000 for the insurance? This means many companies would have a sizable financial incentive to simply drop the insurance.

So then what happens? What happens to these folks who previously had the insurance the President said they could keep? Of course, we all know they can't because, once again, the President misled the American people—I believe intentionally. Well, then these employees who were dropped would have to enroll in a government-run exchange. So what happens in the exchange? Well, many of these individuals would qualify for subsidies from the Federal Government to help them purchase insurance—subsidies from the Federal Government to help them pay for insurance that they were previously getting

at work, but now because of the health care law they can't get it anymore.

So who is going to end up subsidizing this? The American taxpayers are now going to be paying for the health insurance instead of the employer. This is not only going to cause many Americans to lose their health insurance, but it will also make the \$1 trillion health care law even more expensive than the Congressional Budget Office said this past week.

Many businesses surveyed stated they do not intend on dumping the health insurance plans, but they said something else. They said they are not going to stop providing it. Instead, employers are saying to workers: If you want to keep this, you are going to have to pick up the additional cost of your insurance coverage, and you are going to have to do it by helping to pay higher copays, higher deductibles, or participating and contributing to the higher premiums we are going to have to pay.

So for those Americans lucky enough to keep their employer-provided coverage, they will now be paying more money for that privilege. This means employees have essentially two alternatives under this health care law. Either they will lose their employer-provided coverage or they will be facing higher insurance premiums.

For over 150 million Americans who receive their insurance through their employer, neither of these choices is a good one. It didn't have to be this way. That is why I remain committed to repealing the President's health care law and replacing it with patient-centered reforms that will allow patients to get the care they need from a doctor they choose at lower cost.

Thank you, Madam President. I yield the floor.

The PRESIDING OFFICER. The Senator from Minnesota.

Ms. KLOBUCHAR. Madam President, I ask unanimous consent to speak in morning business for up to 15 minutes.

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

Ms. KLOBUCHAR. I am here to talk about two very different subjects, two very different bills. One is the farm bill, and one is the Violence Against Women Act. Both bills are stuck over in the House of Representatives, and both bills should pass. Both bills received significant bipartisan support in the Senate. I am simply asking my colleagues in the other body to get their job done and to get these bills passed.

THE FARM BILL

I will start with the farm bill. Minnesota is fifth in the country for agriculture. It means a lot to our State, it means a lot to the rural areas, but it is also tied to our metropolitan area with our farm businesses, with our food producers, and it is clearly tied in with the rest of the country. This spring's talk of a bin-busting crop has burned away under the extreme summer heat. Farmers and ranchers across the country are experiencing what the U.S. De-

partment of Agriculture is calling the most widespread drought we have seen in decades.

With nearly 90 percent of the corn and soybean crops being grown in areas impacted by the drought, the crop losses are being felt not just by our grain farmers but also are driving up feed prices for our livestock, poultry, and dairy producers. As we well know, dairy producers have already come off some very difficult years.

Higher feed costs for cattle, pork, poultry and dairy impact all Americans at the grocery store. Yesterday the USDA estimated that consumers could expect to pay 3 to 4 percent more for groceries next year at this point.

While some people might think that food magically appears on their tables or in their grocery stores, in Minnesota we know food is produced every day by our farmers. Farmers stand behind each General Mills box of Cheerios or every Jennie-O turkey on the dinner table. That is why when I travel our State I am always reminded of the critical role farming plays in our State's economy and in our country's economy. It has, in fact, been one of the brightest spots. Minnesotans in rural communities and larger cities all benefit from a strong farm economy that provides jobs at farms, mills, processing plants, and equipment manufacturers.

While Congress can't do anything about the lack of rain, we shouldn't make this disaster worse by delaying the passage of the farm bill, which gives farmers and ranchers the assistance they need to help weather this disaster and the certainty they need to make plans for next year and the year after and the year after that. The fact that the 2008 farm bill was a 5-year time period was key to the stability in the rural areas. It was key so farmers could plan ahead. It made a difference during the downturn. We need to do that same thing again.

I think it is a mistake for the House leadership to delay further action on the farm bill. These bills are never easy, but in the Senate we were able to work through 70 amendments before passing the bipartisan farm bill with a strong 64-to-35 vote. Maybe they should do the same.

As part of our responsibility to do more with fewer resources, this bill includes over \$23 billion in cuts over the 2008 farm bill. We eliminated direct payments, further focused farm payments on our family farmers, and worked to eliminate fraud and waste through the farm bill to ensure these programs are efficient and targeted.

President Eisenhower was famously quoted as saying this:

Farming looks mighty easy when your plow is a pencil and you're a thousand miles from the corn field.

I fear that some in Washington have taken that same position and are content with kicking the can down the road and leaving rural America in the lurch. Well, those of us in the Senate

who supported this bill—Democrats and Republicans—were not content with putting our heads in the sand. We weren't content with just letting the crops burn out in the fields. We wanted to get something done.

There are those in the House, such as Representative COLLIN PETERSON of Minnesota, who are trying valiantly to get this farm bill through the House. We must let them do this.

The Senate passed the 5-year farm bill because it is important. It is important because it strengthens the crop insurance program, it funds livestock disaster programs for this year, and continues the program through the end of the farm bill. It ensures that the programs farmers use to get help through tough times, such as the emergency financing credit program or disaster grazing authorities, will be continued with unbroken service.

The farm bill also includes two of my amendments that will help farmers get through these tough times. The first amendment reduces the cost of accessing crop insurance by 10 percent for beginning farmers. This is critical because beginning farmers are less able to afford crop insurance protection and are under greater financial stress because of the drought.

The second amendment eliminates the penalty for beginning farmers that graze livestock on CRP land. This will help beginning ranchers struggling with high feed prices and will also benefit all livestock producers by freeing up the corn to be fed to other animals.

Secretary Vilsack is working at the USDA to help producers with this drought. Under his leadership, the USDA has streamlined the disaster declaration process, reducing the time it takes to start getting help for impacted counties by 40 percent. They reduced the interest rate for emergency loans, as well as reduced the penalty for producers grazing livestock on conservation reserve program acres from 25 down to 10 percent.

While these are important steps, they in no way replace the help farmers in this country will get from this farm bill. We all know it is not just a farm bill, it is a food bill. Only 14 percent of this that we look at is farm programs. The rest are conservation programs. The rest are important school lunch programs. This is a farm bill for the country not just the rural areas. But we can see—anyone who drives through Wisconsin, anyone who drives through Indiana or Missouri or Iowa can see—firsthand why we need this safety net for our farmers, why we need this safety net for our country.

We plead with the House to get this done, to follow the leadership of COLLIN PETERSON and those of us in the Senate who, on a bipartisan basis, got this farm bill done. They need to take it to the floor.

VIOLENCE AGAINST WOMEN ACT

Madam President, as I mentioned, there is a second bill that has also been hung up, a bipartisan bill that received

significant support in the Senate—in fact, it got the support of every single woman Senator in this body, Democrat and Republican—and that is the Violence Against Women Act.

Here in the Senate we passed that reauthorization bill in April on a bipartisan 68-to-31 vote. Getting to that point was a tough road. It was not always clear we were going to pass the bill. Just like the two reauthorizations from 2000 and 2006, our bill strengthens current law and provides solutions to problems we have learned more about since the Violence Against Women Act was first passed in 1994. Ever since then, this bill has been able to get through both Houses on a bipartisan basis without significant controversy.

We do not want to go back in time. We do not want to go back to a time when we treated women who were victims of domestic violence like they were not really victims, like it was something they should just expect to happen. We do not want to turn back on the great strides we have made.

One of the improvements in this current bill focuses on a particularly underserved community: women living in tribal areas. We have a number of reservations in Minnesota, and it is a heartbreaking reality that Native American women experience rates of domestic violence and sexual assault that are much higher than the national average.

Our committee, the Judiciary Committee on which I serve, worked closely with the Indian Affairs Committee to come up with some commonsense solutions to the horrific levels of domestic violence and sexual assault in tribal areas.

One of the problems on tribal lands is that currently tribal courts do not have jurisdiction over non-Indian defendants who abuse their Indian spouses on Indian lands, even though more than 50 percent of Native women are married to non-Indians.

The bipartisan Senate bill addresses this problem by allowing tribal courts to prosecute non-Indians in a narrow set of cases that meet three specific criteria: the crime must have occurred in Indian Country; the crime must be a domestic violence offense, and the non-Indian defendant must live or work in Indian Country.

That is the way we get these cases prosecuted. I do not think we believe the Federal courts are going to come in and handle all these domestic violence cases. This is the pragmatic solution that protects these Native American women.

As we were considering the Violence Against Women Act on the Senate floor, many of us had to work very hard to get the message out there that VAWA was and always has been a bipartisan bill—one that law enforcement and State and local governments strongly support.

Throughout this entire process, under the leadership of Senator LEAHY and Republican Senator CRAPO, who

did this bill together from the beginning, I have found it very helpful that whenever I needed to tell people why we needed to pass a reauthorization bill, I could point to the great work that my State is doing to combat domestic violence.

There is the legacy of Paul and Sheila Wellstone, who were there at the beginning ushering this bill through in 1994.

Minnesota is the home to many nationally recognized programs.

The Hennepin County Domestic Abuse Service Center that I was honored to be in charge of during my 8 years as county attorney in Hennepin County is a nationally recognized center. We opened one of the first shelters in the country in 1974, and the city of Duluth was the first city to require its police officers to make arrests in domestic violence cases.

I have learned about a unique domestic violence court that Stearns County—that is the area around St. Cloud—has implemented using money from VAWA grants. The partnership, which involves trained people from all levels of the criminal justice system, has allowed 58 percent of the victim participants to separate from their abusers.

Washington County relies on cutting-edge research to provide direction for officers to take appropriate action when responding to domestic violence calls. It is the only program of its kind in the entire country.

These are the kinds of innovative initiatives from law enforcement that are especially critical to combating violence and are directly a result of the Domestic Violence Against Women Act that we have worked so hard to pass in past years in this Congress.

I want to stress just how crucial it is that we get this bill signed into law. We have made a lot of progress over the years, and we have been able to work together across the aisle to build on VAWA's successes. But we should not just send any bill to the President. As you know, the House has passed its own reauthorization of VAWA, which, unfortunately, does not include many of the improvements the Senate bill includes, including the one I mentioned on tribal courts. It also rolls back some of the important improvements that have been made to VAWA in the past.

I am hopeful we will be able to iron out these differences as we move forward, but I strongly believe the improvements that were included in the Senate bill should remain a part of the bill that gets sent to the President. I hope our colleagues in the House will follow suit with the Senate on this domestic violence bill, pass a bipartisan bill, get this done, and get it done soon. It simply is not that hard. Just look into the eyes of a domestic violence victim, look into the eyes of the children, and you know it is not that hard. I yield the floor.

THE PRESIDING OFFICER. The Senator from Arizona.

Mr. KYL. Madam President, I just want to make a very brief comment

primarily for the benefit of our Republican colleagues who have been inquiring about whether we would have, and when we would have, a vote to invoke cloture to proceed to the cybersecurity legislation.

I am hopeful we can do that very soon. From my perspective, it would be wise for us to move forward, to go to the bill, and see if we can work things out. There have been discussions between various groups who are interested in the subject. They are now all talking to each other, which is a very good sign because it is amazing how, when Senators get together and talk to each other, sometimes we can actually accomplish things in a bipartisan way.

So my hope is that we can do that. If it turns out it does not work out, we can always vote no at the end of the day. But I believe we should go forward, that we should get on the bill, and, therefore, I intend to support cloture on the motion to proceed to the cybersecurity legislation.

I thank my colleagues for yielding.

The PRESIDING OFFICER. The Senator from Texas.

Mr. CORNYN. Madam President, I appreciate the courtesy of my colleague from Maryland, and I promise I am going to be just no more than 10 minutes.

TAX HIKES AND SMALL BUSINESS

Two years ago, Members of both parties in this Chamber recognized that America's economic recovery was fragile, too fragile to absorb a tax increase. Since then, obviously, my colleagues across the aisle have changed their minds and experienced a change of heart.

Yesterday the Senate voted to raise taxes. I have been amused by some of the headlines I have read that say the Senate voted to cut taxes, which is false. The Senate did not vote to cut taxes; the Senate voted to maintain the tax rates that have been in existence for 12 years for a certain class of taxpayers, while raising taxes on everyone else.

I cannot explain the logic behind this vote. I can only assume it is some election-year calculus designed to galvanize the political base of our friends across the aisle. It most definitely is not good economics, and it is not good for job creation.

For 3 years, it is no secret America has been living through the weakest economic recovery since the Great Depression. We know from history, from economics, and from common sense that the last thing you want to do amid persistently slow economic growth is to dramatically raise taxes on income and investment. If you want more economic activity, if you want growth, then you do not burden it further. You relieve those burdens, which allows it to flourish and grow, which creates prosperity and jobs. Yet our friends across the aisle just voted to raise taxes on nearly 1 million American businesses.

Many American businesses do not operate as a corporation. They operate as

a sole proprietorship, a partnership—in other words, a mom-and-pop operation—or even as a subchapter S or some other legal entity, which causes business income to be paid on individual tax returns not on a separate corporate tax return.

The bottom line is, when we raise taxes on people in the top tax brackets, we inevitably are going to capture, in this instance, 1 million different individuals paying business income on an individual tax return, which is bad for the economy, bad for jobs.

We should make no mistake about it: Given our anemic growth rates, given the ongoing debt crisis in Europe, and given the economic slowdown in China and other emerging market countries, raising taxes on so many job creators could easily tip the U.S. economy back into recession. If we take yesterday's vote to increase taxes on so many small businesses together with the unwillingness to deal with the single largest tax increase in American history—which will occur on December 31, 2012, and is something that has been called taxmageddon, when virtually all the tax provisions in the code will expire, the ones passed 12 years ago—if we combine that huge tax increase with the sequestration, \$1.2 trillion, which comes disproportionately out of defense spending, without exception the economists I have talked to say we will be in a recession.

Why is it that our colleagues across the aisle are willing to risk putting America back into recession just to raise taxes? I cannot understand that, unless they have taken some kind of poll, done some sort of focus group that has laid out some strategy which is not readily apparent to most people.

So the idea that this tax increase would solve our fiscal problem is laughable. As my good friend, the Republican leader, said yesterday, the additional revenue generated by the taxes that our Democratic friends voted for yesterday “[wouldn't] even fund the government for a week.” A week—and that is before we consider the harmful impact on the economy and jobs.

Whenever I talk to business owners back home in Texas, they express utter bewilderment as to why Members of Congress would want to raise taxes during the current economic environment. Don't our friends across the aisle realize how many small businesses are struggling to stay afloat? Don't they realize that our Byzantine Tax Code and misguided regulations are already strangling job creation? Don't they realize our national unemployment rate has been stuck at more than 8 percent for 41 consecutive months?

No one here wants to see another recession, but apparently some are willing to risk a recession by putting ideology ahead of sound economic policy. After last night's vote, I thought of all the Texas entrepreneurs—more than 400 of them—who have contacted my office, sending their personal, inspiring American success stories. These stories

remind us that the American dream is still alive, and it is inextricably intertwined with our free enterprise system. It is not a gift from government. It is what people earn as a result of hard work and the opportunities given to them in this great country.

These stories remind us the American dream is not dependent upon government assistance. It is not about taxing certain people to pay for ideologically driven government projects like Solyndra. It is about offering all Americans the opportunity to earn their success and achieve their dreams.

My office has received literally hundreds of entrepreneurial success stories from Texas, stories such as that of Gary Murray, a Vietnam veteran who came home from the war after three tours as a marine in Vietnam, who spent two decades working at IBM and then launched his own fencing club—a fencing club. For more than a quarter century, Gary's Round Rock Fencing Club has been training young Texans and producing world-class talent, including two Olympians, one world champion, and eight national champions. It is a remarkable story about someone deciding this is what they wanted to do, this is where their passion lies, making the most of it, and creating opportunities for other people.

Gary started the Round Rock Fencing Club with his own money, without any financial support from the government. What he achieved, he achieved on his own. His story is a testament to hard work and human creativity. As Gary puts it: “The only support I ever got was from my wife and family.”

There are many other business owners like Gary Murray all across Texas and all across this great country.

Before my colleagues advocate higher taxes on these businesses, perhaps they should spend some time talking to the job creators and small business people and the entrepreneurs about the myriad challenges and obstacles government places in their way because of high taxes and overregulation. I suspect my colleagues might learn something.

I yield the floor.

The PRESIDING OFFICER (Mr. SANDERS). The Senator from Maryland.

AFFORDABLE CARE ACT

Mr. CARDIN. Madam President, I have taken the floor before to talk about the health care reform bill, to comment on the Supreme Court decision, which I believe history will show was clearly the right decision. It was the right decision on the law giving the Congress the power to legislate in an area where there is a national need, as the legislature did in the 1930s with Social Security and in the 1960s with Medicare.

The health reform proposals that were adopted by Congress are within the purview of the legislative branch of government. The Supreme Court upheld that right in that decision. I also said it was the right decision because it allows us to move forward on

a path toward universal coverage, where all Americans are guaranteed access to affordable health care. America will now join all of the other industrial nations of the world to say health care is a right, not a privilege.

The legislation that was passed, the health reform bill, has already helped American families. Let me talk about an area—I could talk about many—about what it has done in protecting our consumers against the practices, the arbitrary practices of health insurance companies. We already are seeing that it is in effect where families are being able to take advantage of the fact there are no longer any lifetime caps on health insurance policies. By 2014, we will eliminate annual caps on benefits on health insurance plans. We already have seen for our children the elimination of preexisting conditions, so our children can get policies without having restrictions on what is covered and what is not covered. By 2014 we will see that the preexisting conditions for everyone will no longer be an obstacle to full insurance coverage. That is particularly important for women, where we know at times they have been held to a preexisting condition because of a pregnancy or being the victim of domestic violence.

We have seen discrimination in premiums against women. That no longer will be the case. I could talk about many Marylanders who are happy today because they can stay on their parents' insurance policies—the fact that they are over the age of 21. They can now stay on that policy until age 26.

I want to talk about one other aspect of this law that may not be quite as familiar to our constituents. This provision will take effect on August 1, but we already are seeing the benefits. What I am talking about is the 80-20 rule, where health insurance companies must give value for the premium dollar to the beneficiary. At least 80 percent of the dollars we pay for premiums must go for benefits.

Let me share with you a letter I received from one of my constituents. She wrote:

I recently had a pleasant surprise. . . . two checks from my health care [insurer] that were rebates on premiums paid. I am someone who has to buy individual health coverage and have been doing so for the last 8 years. The premiums are high and the deductible is high—so I am essentially paying a high price for catastrophic coverage while still paying for individual doctor visits, prescriptions, etc. It is frustrating, but the choices are limited and expensive for individual coverage, and you don't really know how good your coverage is because you don't use it unless you have a major medical event. My premiums go up every year despite the fact that I don't file claims. This month I received a check in the amount of \$139 from my current [insurer] and over \$300 from a previous [insurer]. Both checks were rebates as a result of the new health care act.

I did not realize it, but the act requires insurance companies to use 80% of the premiums they collect on health care costs. . . . and neither of them hit that percentage and

were thus required to provide a refund. Wonderful! The bill is so complicated that I do not understand a great deal of it—but am very pleased with this aspect which seems to go a long way in helping keep health care costs reasonable and prevent consumers from being gouged. . . . So thanks to the Senator and all who helped with this health care act.

I bring this to my colleagues' attention, because there are going to be millions of American who are going to be getting rebate checks, and some are going to start scratching their heads, wondering where it is coming from. They are going to be saying: Gee, I guess I made a mistake in the premiums I paid. They are returning them. They are getting those checks because of the passage of the health reform bill, and the provision in the health reform bill that requires insurance companies to give value for the premium dollars we pay.

That protection is now the law of the land. Thanks to the acts of Congress and President Obama, and the Supreme Court upholding the law, those rebates are going to be received. The number of people in the country is 12.8 million Americans who are going to get rebate checks worth about \$1.1 billion. Average rebate: \$151. That is real money for people who are struggling with their health care needs.

I am proud that in the State of Maryland, there is going to be \$27 million made available to 141,000 Marylanders, with an average rebate of \$340 for those who get rebates in my State. Let me break this down a little bit further. In the individual market, like the person I received the letter from, the rebates for the people in Maryland will actually average a higher amount. They will average \$496. I think that speaks to the fact that insurance companies have hedged their bets in the individual market. They tell us that, you know, we have got to charge a lot more because we do not know what we are getting, when in reality they are making a lot more money in the individual market.

So for the people of Maryland, 38,000 of them are going to get, on average, close to \$500 in rebates thanks to the passage of the Affordable Care Act, thanks to the passage of health reform, and thanks to the Supreme Court upholding our right to do it.

The same thing is true in the small group markets where we find that there will be 3.3 million Americans getting rebate checks who are in the small group markets. These are the markets, of course, in which again the options were not as great, more difficult, because of insurance carriers not being as anxious to insure people in small group markets as they are in the larger markets.

The average rebate per family will be \$174. In Maryland that number again is higher, \$310 for the 13,000 people in Maryland. It also applies to those in the large group markets. These are the large plans. They also are going to see rebates because the insurance carriers charged excessive fees. And they are

going to get premium dollar rebates. Some 5.3 million Americans in these large plans will see rebates that average \$135. In my State of Maryland, it will be 89,000 people, with rebates averaging \$268 a family. These are 1-year numbers. These continue every year. So let me tell the people of Maryland and the people of this country what you can expect. You might get a check that will be delivered to you in the mail. It will be a rebate check. That is as a result of the passage of the health reform bill. You might also see a deposit into the account that automatically pays for your health premiums, because the insurance carrier can make a direct deposit into the accounts which are paying for these premiums.

It is possible you might find a reduction in future premiums. They can use it to reduce your future premiums, but they have to let you know that, so you realize you are getting the rebate, but it is being applied against future premiums. Or if the employer is paying the premiums, the rebates will go to the employer, but the employer must use it to benefit your plan. They cannot use it for themselves. It is used to help again the beneficiary. You will get notice of that.

My purpose again is to make it clear that you would not have gotten these rebates but for the protections that are in the Affordable Care Act. I know my colleague from Vermont and I have been on the floor many times pointing out that all Americans, not just those who do not have insurance today, not just those who might have been discriminated against because of preexisting conditions, not only that 24-year-old who is now on her parent's policy, but all Americans have benefited from the Affordable Care Act, the protections that are in it.

Now millions who thought they were being treated unfairly by their insurance companies are going to be able to get rebates because of excessive premiums. The rule works in combination with another provision of the law that requires rate review to ensure premium increases are reasonable. In other words, we have put into the law protections against unreasonable increases in your premiums. Insurance companies are now required to justify any premium increases of 10 percent or higher. Most States now have the authority to determine whether these increases are excessive, while HHS reviews rates in States that do not operate under effective rate review programs.

That is how federalism should work. States have an opportunity to act. If they do not have adequate review, we have national backup and protection to make sure the rate reviews are being handled in the appropriate way. So as our constituents start to get the benefits—another benefit of the health reform bill, and there are many more that are starting to take effect, and we will hear about some more of those next week, on August 1—I wanted my constituents of Maryland and my

friends around the Nation to know we have provided that you get value for the premium dollar you pay for your health insurance.

We back that up with enforcement, so if there are excessive premiums being charged, the insurance carriers must rebate those premiums to you. Millions of Americans will get the benefit, starting now. We are pleased that this type of protection is in the Affordable Care Act.

I yield the floor and I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The assistant legislative proceeded to call the roll.

Ms. STABENOW. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

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

THE FARM BILL

Ms. STABENOW. Mr. President, I wish to take a few moments to update folks about what is happening as it relates to the very important effort to pass a 5-year farm bill for our country—for our ranchers, for our farmers, for those who care deeply about nutrition and conservation policy for the country.

We have somewhere between 16 and 20 million people who work in this country because of agriculture—the farm bill and food policy—and I am very proud of all the work we did together to pass a bipartisan farm bill. In doing that, we sent a very strong message on a number of fronts that we were committed to economic certainty for our growers. We said we understand the need to have long-term policies in place, and we also sent a message about disaster assistance.

I have spoken on the floor before, as my colleagues have, about the very serious situation happening all across our country as it relates to livestock and the broad question now of drought in every region of the country. We also have had areas, in addition to drought in Michigan and other places, where food growers have been hit with an early warming and then a freeze again. So we have had multiple reasons to care about short-term disaster assistance, and I am very proud the bill we passed includes a very good livestock disaster assistance program available for this year which will be very helpful for our livestock producers.

We also added provisions for fruit growers that will help those who don't have access to any crop insurance. That will not only include this year, but we looked to the future by putting in new options on crop insurance, new tools for the risk management agency to develop with growers, with commodity groups across the country crop insurance for the future. So as we see these kinds of weather disasters, they will have more certainty because there will be better coverage and broader kinds of coverage for crop insurance for all commodities, which we don't have today.

We definitely need to pass a farm bill. We need the House to pass a farm bill both for long-term policy but also for disaster assistance right now, and we know this is an opportunity to achieve deficit reduction. The only bipartisan effort we have had on deficit reduction on the Senate floor—and I would argue probably bipartisanship on the House floor as well—has been through the farm bill, with \$23 billion in deficit reduction, with major reforms, changes in policy, and eliminating four different subsidies that are there when growers don't need them or for things they don't plant anymore and replacing that with a risk-based, market-based system for when farmers truly do need us, as they do now.

So there is a whole range of things we have done—reforms and strengthening conservation efforts in our country, focusing on the right policies around nutrition, around local food systems and so on—and all that is in jeopardy at the moment because the House, rather than bringing to the floor the bill passed out of the House committee, which, even though it is different and I would argue doesn't have all the reforms we have and takes a little different approach on commodities and so on, it is a bill we can work with to come to final agreement on between the House and the Senate. But instead of bringing that to the floor, getting it done, we are now hearing discussions about just passing some kind of a disaster assistance program.

Certainly, we need to do that. We have already passed it and we can strengthen it as we move forward to a conference committee and I would support doing that as well. But instead of having a full 5-year farm bill policy, they are talking about kicking the can down the road one more time. That seems to be a very popular strategy around here. It is not one the public wants us to use. They want to extend the farm bill for another year, with no deficit reduction, no reform, no certainty for farmers, and with policies extended another year that don't work for a lot of industries and then just do some disaster assistance. I think that would be a disaster.

I know we have colleagues on both sides of the aisle—and I am grateful for the leadership of the chairman and ranking member in the House for their advocacy and leadership—who want to get this done, but we need to know the House leadership will allow that to happen so we can get real reform, deficit reduction, and the kinds of policies we need in place that will solve problems and provide the safety net all our farmers need. If we end up in a situation with just an extension, what happens? As our distinguished Presiding Officer knows, it would keep in place for another year a dairy policy that doesn't work.

I remember, in 2009, sitting around the table and talking about what was happening to dairy farmers—folks going out of business, losing their

farms because of policies that didn't work. Now the House is talking about extending those policies for another year rather than adopting the changes and the reforms we have put in place that would help dairy farmers all across the country. They are talking about an extension that would eliminate about half the support for fruit and vegetable growers that we put in place. In the last farm bill, I was proud to offer that, and we strengthened that in this farm bill. It is one of the largest areas of commodities, groups of commodities, in the country. So that would not be continued.

There are a number of things that, frankly, would not be continued or available, and there are a number of things that would continue that are bad policy. So if we have a 1-year extension, we are continuing something we rejected and that everybody on both sides of the aisle in the House and Senate said they didn't want to do, which is direct payments going to farmers, government payments, regardless of whether the prices are high or low, in good times or bad times, and continuing even on things that aren't grown anymore. We all said that makes no sense.

We all said, instead, that we wanted to move to a risk-based system and have a strong safety net there when farmers and ranchers need us, to strengthen crop insurance and make sure farmers have skin in the game; that they are sharing in the cost on crop insurance.

But none of that happens with a simple 1-year extension. We continue things we have all said are not good policy, that cost taxpayers money, and that we shouldn't be spending our money on at a time of huge deficits; that we should not have those kinds of subsidies in place. We eliminated four of those, with \$15 billion in savings alone in the commodity title. All that would go away under what the House is talking about. We would be continuing things people have said were bad policy. Everyone talks about reforms and changes, but this would continue the old ways.

We eliminated about 100 different programs, duplication, and things that do not work anymore—redundancy, whatever it is. About 100 different programs we eliminated in what we passed. They would all continue—every single one of them—for another year if we just do a 1-year extension.

Let me just say in conclusion that I encourage House colleagues to join with us. We can have differences in what our commodity title looks like, and I respect those differences. We can work those out if we have the opportunity to negotiate in good faith and get things done. We will do that. We can have differences in what should happen in the nutrition title, but we should not be saying to farmers and growers that we are going to walk away from them and put in place another kick-the-can-down-the-road

strategy that keeps bad policy or no policy going, no deficit reduction, and puts us in a situation where, frankly, 1 year from now it is tougher and it is a bigger mess than ever, with our growers trying to go to the bank, trying to figure out what they are going to do when planting season comes and making decisions, all the while looking at us and asking: What happened here? Why did you do this?

We did our job in the Senate on a strong bipartisan basis. It was a lot of hard work. We spent a lot of time here. We need to complete the job. If our House colleagues will come together with us; if the Speaker, the leadership in the House, will decide to give us a vehicle with which to do that, I am very confident we can get the job done.

I yield the floor.

The PRESIDING OFFICER. The Senator from Connecticut.

Mr. LIEBERMAN. Mr. President, for the information of my colleagues, I know the Senate majority leader is in discussions with the Republican leader, and I know the hope is we can soon have the vote on a motion to proceed to S. 3414. But as yet I have not been informed there has been the necessary meeting of minds. I hope it will be soon, and I hope everyone will support it.

I yield the floor, and I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. HOEVEN. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

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

(The remarks of Mr. HOEVEN pertaining to the introduction of S. 3445 are located in today's RECORD under "Statements on Introduced Bills and Joint Resolutions.")

Mr. HOEVEN. I suggest the absence of a quorum.

The PRESIDING OFFICER (Mrs. SHAHEEN). The clerk will call the roll.

The legislative clerk proceeded to call the roll.

The PRESIDING OFFICER. The Senator from Vermont.

Mr. SANDERS. Madam President, I ask unanimous consent that the call of the quorum be rescinded.

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

THE ECONOMY

Mr. SANDERS. Madam President, there has been a lot of talk about one of the major issues we as a nation are going to have to deal with, and certainly the Presidential candidates will be talking about it during the next few months, and that is that we have a \$16 trillion national debt and we have a \$1 trillion deficit. I think all Americans understand this is a very important issue, and it is something we as a nation are going to have to grapple with.

How we deal with the deficit and the national debt is certainly one of the

most important and interesting issues we are going to have to address.

What I find interesting is that when we talk about the deficit and the national debt, there seems to be, among some of my colleagues, collective amnesia. It is as if this debt and deficit popped up yesterday and we have no understanding of how we got to where we are today.

I would like to take a moment to remind some of my friends that back in January of 2001—not so many years ago—when President Bill Clinton left office, this country was not running a deficit, it was running a very significant surplus of some \$236 billion. That is a very significant surplus. As a matter of fact, in 2001 the Congressional Budget Office projected that we would have Federal budget surpluses totaling \$5.6 trillion from 2002 to 2011. In other words, when Clinton left office there was a very significant surplus, and the projection was that surplus was going to go up and up. What happened? Well, that is a question we need a little bit of time to discuss.

I find it interesting that there is no context for deficit reduction. Let me suggest that, in fact, some of the people who come down to this floor and talk the loudest about the deficit and the national debt are precisely those same people who caused the national debt of \$16 trillion and a deficit of over \$1 trillion.

How did we get to where we are today from the time when Clinton left office and we had a significant surplus? No. 1, many of our deficit hawks who are coming down to the Senate floor telling us about all the programs we have to cut for the middle class, working families, our children, and the elderly, are real deficit hawks. My goodness. When it came to the war in Iraq, many of us voted against it since it didn't make a whole lot of sense. We also noted that our deficit hawk friends went to war—I believe for the first time in the history of America—and forgot they would have to pay for that war. I think some of us might hold a little bit of doubt in some of the comments of our friends about their real sincerity and concern about deficit reduction when they went to a war in Iraq which will end up—after we take care of the last veteran wounded in that war 80 years from now or whenever—costing probably \$3 trillion.

Well, if you spend \$3 trillion to go to war, forget to pay for it, and then come to the Senate floor and tell us how concerned you are about the deficit and the national debt, some of us are saying: Well, maybe that is not the case. Where were their concerns about the deficit when they went to war when we had a deficit hawk President named George W. Bush? So that is one of the major reasons we are running a \$1 trillion deficit right now.

The second reason is—and you don't have to have a Ph.D. in economics to understand it—that if in the middle of a war they decide to give huge tax

breaks, including \$1 trillion over a 10-year period to the top 2 percent, the billionaires and millionaires, so \$1 trillion is not coming into the Federal Government, that adds to the deficit. I ask my Republican friends where was their concern about the deficit and the national debt when they gave \$1 trillion in tax breaks to millionaires and billionaires?

The third point I wish to make is that we are in the middle of a horrendous recession. Unemployment is sky high and underemployment is sky high. People have lost homes and their life savings. People are hurting. This recession was caused by the efforts—and I must confess, not just a Republican effort but also a Democratic effort—and the bipartisan desire to deregulate Wall Street because people believed that if we deregulate Wall Street and allow insurance companies to merge with commercial banks and investor banks and we do away with Glass-Steagall, my goodness, those folks on Wall Street—honest people with great integrity—would just create wealth for all Americans. That is what Alan Greenspan, Robert Rubin, and all these guys were telling us. I was a member of the Financial Services Committee in the House and never believed that for one moment. It never made an iota of sense to me. Anyway, these guys fought for deregulation. We had deregulation, and as a result of the greed, recklessness, and illegal behavior on Wall Street, we were plunged into the terrible recession we are in now.

One of the points that are very rarely made on the Senate floor is that today, at 15.2 percent as a percentage of GDP, revenue is the lowest in more than 60 years. So it is easy for people to come to the Senate floor and say we have to cut, cut, cut. They forget to tell us that as a result of the Wall Street-caused recession, at 15.2 percent, revenue is the lowest as a percentage of GDP in more than 60 years. That is an issue we have to deal with.

You know what, we don't increase our revenue when we give more tax breaks to billionaires. We don't increase our revenue when we say that at a time when we have tripled military spending since 1997, maybe we need even more for the military. That is not a way to reduce the deficit.

Now, what do my Republican friends and some Democrats say? Well, they come to the Senate floor and suddenly—after going to war without paying for it, after giving huge tax breaks to the rich, after deregulating Wall Street—realize we have a deficit problem, and they are very concerned about this deficit problem. They come to the Senate floor and say: The only way we can go forward is to cut Social Security. Social Security is funded independently. It hasn't added one nickel to the deficit, but we are going to cut Social Security anyway. We are going to cut Medicare, we are going to cut Medicaid, we are going to cut Pell grants, we are going to cut education,

and we are going to cut environmental protection. That is deficit reduction.

Are we going to ask millionaires and billionaires, who are doing phenomenally well, whose effective tax rate is the lowest in decades, to pay one nickel more in taxes? No, we can't do that, but we can cut Social Security, Medicare, Medicaid, education, and every program that the children, seniors, and working families of this country depend upon.

Now, to add insult to injury in terms of this movement supported by big-money interests that have so much influence over what goes on here in Congress, it is important to look at the playing field of the American economy today to understand what is going on. Are the people on top really hurting and suffering? Are large corporations today really struggling under onerous corporate taxes? The answer is, obviously not.

We don't talk about it enough, and too few people even mention it, but I do, and I will continue. It is important today to understand that the United States has the most unequal distribution of wealth and income since the 1920s and the most unequal distribution of wealth and income of any major country on Earth. Why is that important? It is important to know that. Before we cut Social Security, Medicare, Medicaid, education, and the ability of working-class kids to go to college, we have to know the condition of how people are doing today. The middle class today is shrinking and poverty is increasing. When we cut food stamps and Medicaid, we are going to hurt a whole lot of people, and in some cases very tragically.

Just last week a member of my staff went to southwest Virginia, and she spent the day at a program in which thousands of people in that area were lining up to get dental and health care because they didn't have any health insurance. There are 45,000 Americans who will die this year because they don't have health insurance and can't get to a doctor in time. There are people who say: Let's cut Medicaid. There are people all over this country who can't find a dentist. There are children who are suffering from dental decay. Let's cut Medicaid. Well, I don't think so.

If we look at the country, the middle class is shrinking, people are hurting, but people on top are doing phenomenally well. Very few people talk about it. I am going to talk about it. In the last study we have seen in terms of income distribution in this country—and that is what happened between 2009 between and 2010–93 percent of all new income created over that year went to the top 1 percent. I will say it again. Ninety-three percent of all new income in that year went to the top 1 percent. The bottom 99 percent had the privilege of sharing the remaining 7 percent. Yet, when we ask the people on top to maybe pay a little bit more in taxes, oh my goodness, there are lobby-

ists all over Capitol Hill saying: We can't afford to. We are down to our last \$50 billion. We just can't afford another nickel in taxes. We need that money now. Thanks to Citizens United, we can pump that money into political campaigns.

One family who is worth \$50 billion is going to put \$400 million into the campaign. Another guy who is worth \$20 billion can't pay more in taxes, but he does have hundreds of millions to pour into political campaigns.

In terms of distribution of wealth, which is a different category of costs than distribution of income, we have an incredible situation. I hope people understand what is going on in this country, where one family—one family, the Walton family, of Wal-Mart—now owns more wealth at \$89 billion than the bottom 40 percent of the American people. One family owns more wealth than the bottom 40 percent. Do we know what some folks want to do here? They want to repeal the entire estate tax and give that family a very substantial tax break, because owning \$89 billion is obviously not enough. They are struggling. We have to give them a tax break while we cut Social Security, Medicare, and Medicaid. If that makes any sense to the American people, I would be very surprised, and it does not make sense to the American people.

According to a February 2011 Washington Post poll, while more than 70 percent of Americans oppose cutting Social Security and Medicare, 81 percent supported a surtax on millionaires to reduce the deficit. My guess is if we go to New Hampshire, Maine, or any other State in America and we say to people, we have a deficit problem and the choice is between cutting Social Security or asking millionaires and billionaires to pay more in taxes, there is, in my view, no State in America—no State in this country, no matter how red it may be—where people will say: Cut Social Security and Medicare and Medicaid, but don't raise taxes on millionaires and billionaires. I don't believe that is true anyplace in America.

Today, the top 1 percent owns 40 percent of the wealth of our Nation while the bottom 60 percent owns less than 2 percent. The top 1 percent owns 40 percent; the bottom 60 percent owns less than 2 percent, and there are Members of this Senate coming to the floor and saying we are going to punish the bottom 60 percent and we are going to give more to the people on top.

There was a study that recently came out that talks about the ability of billionaires and corporations to use tax havens. What we know—and I am a member of the Budget Committee—is that millionaires and billionaires and corporations in this country are avoiding paying about \$100 billion every single year by using tax havens in the Cayman Islands, in Bermuda, Panama, and other countries. Maybe, just maybe, before we cut Social Security

and Medicare, we might want to pass legislation to make those people start paying their fair share in taxes and do away with those tax havens.

Let me conclude by saying we are in a pivotal moment in American history. If we as a Nation do not get our act together, in my view, we will move even more rapidly in the direction of an oligarchy, where we will have a few people on the top with incredible wealth controlling not only our economy but also, through Citizens United, the political life of this country. We are seeing that playing out right here on the floor of the Senate, with people who are turning their backs on working families and the middle class, and at a time when the wealthiest people are doing phenomenally well, fighting for more tax breaks for people who absolutely don't need them.

I hope the American people pay rapt attention to this debate, and I hope the American people get involved in this debate, because if they do not, mark my words, within 4 months, a handful of people, supported by corporate America and the big money interests, are going to bring down to this floor a deficit reduction proposal which will cut Social Security, Medicare, Medicaid, and give more tax breaks to the wealthiest people in this country. It will have virtually all Republican support. It will have some Democratic support. If we don't aggressively oppose this approach, that is exactly what will happen.

I yield the floor.

The PRESIDING OFFICER. The majority leader.

Mr. REID. Madam President, I appreciate my friend yielding, my dear friend from Vermont.

EXECUTIVE SESSION

NOMINATION OF ROBERT E. BACHARACH TO BE UNITED STATES CIRCUIT JUDGE FOR THE TENTH CIRCUIT

Mr. REID. I ask unanimous consent that the Senate proceed to executive session to consider Calendar No. 759, the nomination of Robert E. Bacharach, of Oklahoma.

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

The clerk will report the nomination.

The assistant bill clerk read the nomination of Robert E. Bacharach, of Oklahoma, to be United States Circuit Judge for the Tenth Circuit.

CLOTURE MOTION

Mr. REID. Madam President, I send a cloture motion to the desk with respect to this nomination.

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

The assistant bill clerk read as follows:

CLOTURE MOTION

We, the undersigned Senators, in accordance with the provisions of rule XXII of the