helping each and every American live a safer and more prosperous life.

Our tasks here in Congress should be straightforward. First, we need to raise the debt ceiling so we can continue to pay our bills and maintain the full faith and credit of the U.S. Government. Second, we need to keep the Federal Government open for business and keep the Federal workers on their jobs. Third, we need to negotiate a comprehensive budget deal that replaces sequestration—a budget that maintains critical Federal investments while spreading the burden of deficit reduction in a fair way and holding Federal workers and their families harmless after subjecting them to so much hardship over the past several months and years. Fourth, we need to reauthorize the Export-Import Bank, a bank that helps us with a level playing field on international commerce, particularly with small companies, and we must reauthorize our surface transportation program on a 6-year reauthorization. You can't do a major highway, bridge, or transit program with a Federal partner that gives only a couple months of commitment. We need to have a multi-year transportation reauthorization passed.

Heretofore, one of the greatest attributes of the American character has been pragmatism. We can acknowledge and respect our differences, but at the end of the day the American people have entrusted us with governing. That means being pragmatic, sitting down, listening to each other, compromising, and providing policies that will stand the test of time. Let us do our job on behalf of all Americans.

Mr. President, I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The senior assistant legislative clerk proceeded to call roll.

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 President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER (Mr. SULLIVAN). Without objection, it is so ordered.

CONCLUSION OF MORNING BUSINESS

The PRESIDING OFFICER. Under the previous order, morning business is closed.

CYBERSECURITY INFORMATION SHARING ACT OF 2015

The PRESIDING OFFICER. Under the previous order, the Senate will resume consideration of S. 754, which the clerk will report.

The legislative clerk read as follows:

A bill (S. 754) to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

Pending:

Burr/Feinstein amendment No. 2716, in the nature of a substitute.

Burr (for Cotton) modified amendment No. 2581 (to amendment No. 2716), to exempt from the capability and process within the Department of Homeland Security communication between a private entity and the Federal Bureau of Investigation or the United States Secret Service regarding cybersecurity threats.

Feinstein (for Coons) modified amendment No. 2552 (to amendment No. 2716), to modify section 5 to require DHS to review all cyber threat indicators and countermeasures in order to remove certain personal information.

Burr (for Flake/Franken) amendment No. 2582 (to amendment No. 2716), to terminate the provisions of the Act after six years.

Feinstein (for Franken) modified amendment No. 2612 (to amendment No. 2716), to improve the definitions of cybersecurity threat and cyber threat indicator.

Burr (for Heller) modified amendment No. 2548 (to amendment No. 2716), to protect information that is reasonably believed to be personal information or information that identifies a specific person.

Feinstein (for Leahy) modified amendment No. 2587 (to amendment No. 2716), to strike the FOIA exemption.

Burr (for Paul) modified amendment No. 2564 (to amendment No. 2716), to prohibit liability immunity to applying to private entities that break user or privacy agreements with customers.

Feinstein (for Mikulski/Cardin) amendment No. 2557 (to amendment No. 2716), to provide amounts necessary for accelerated cybersecurity in response to data breaches.

Feinstein (for Whitehouse/Graham) modified amendment No. 2626 (to amendment No. 2716), to amend title 18, United States Code, to protect Americans from cybercrime.

Feinstein (for Wyden) modified amendment No. 2621 (to amendment No. 2716), to improve the requirements relating to removal of personal information from cyber threat indicators before sharing.

SENTENCING REFORM AND CORRECTIONS ACT

Mr. CORNYN. Mr. President, it is easy for the public and the press to focus on the issues that divide us in Washington, DC, and around the country. In fact, in Washington, DC, that is a world-class sport—focusing on division, the things that separate us, the things where we clearly can't agree, on occasion—but today I am happy to highlight an area marked by broad consensus and true bipartisan spirit.

In my time in the Senate I have learned that neither political party can get what they want done if they try to do it alone. The only way things happen are when consensus is achieved, and that takes a lot of hard work, a lot of cooperation, and a lot of collaboration. If your goal is 100 percent of what you want or nothing, my experience is you get nothing here.

I know ''compromise'' sometimes is a dirty word in today's lexicon. I was just rereading a quote from Ronald Reagan, somebody conservatives look to as an example of the iconic conservative leader. He was pretty clear that if he could get 75 to 80 percent of what he wanted to achieve, he would say: I will take it, and I will fight about the rest of it another day.

But the good news is we have found a way, amidst a lot of the division and polarization here, to achieve a bipartisan coalition on some important criminal justice reforms. Last week I stood with a bipartisan group and introduced the Sentencing Reform and Corrections Act of 2015. This has literally been years in the making, and it was a proud and consequential moment for the Senate.

This week we have kept that momentum going. Senator GRASSLEY, chairman of the Judiciary Committee, held a hearing Monday to discuss the new bill with various stakeholders, and tomorrow the Judiciary Committee will vote on sending the bill to the full Senate for consideration.

This legislation is long overdue and a major step forward for the country. Similar to other successful efforts—and particularly those that inform my actions in the Senate—I look to experiences in the State and what has been tried, tested, and found to work and how it might apply to our job here at the national level.

Back in 2007, in Austin, legislators were confronting a big problem. They had a major budget shortfall, an overcrowded prison system, and high rates of recidivism—repeat criminals—or as one former inmate referred to himself in Houston the other day at a roundtable I held, he called himself a frequent flier in the criminal justice system. I think we all know what he meant. But instead of building more prisons and hoping that would somehow fix the problem, these leaders in Austin decided to try a different approach. They scrapped the blueprints for more prisons, and they went to work developing reforms to help low- and medium-risk offenders who were willing to take the opportunity to turn around their lives and become productive members of society.

I think we would have to be pretty naive to say that every criminal offender who ends up in prison is going to take advantage of these opportunities. They will not—not all of them will, but some of them will. Some of them will be remorseful. Some of them will see how they wasted their life, the damage they have done to their families, including their children, and they will actually look for an opportunity to turn around their lives after having made a major mistake and ending up in our prisons.

In my State, we have a pretty well-deserved reputation for being tough on crime. I don't think anybody questions that, but we also realize we need to be smart on crime, and we need to look at how we achieve the best outcomes for the taxpayers and for the lives which can be salvaged and made productive through their hard work and the opportunity we have provided to them. We also realized that even though incarceration does work—I don't think anybody can dispute the fact that when somebody is in prison, they are not committing crimes in our communities and across the country—but here is the rub: One day almost all of them will be released from prison. The question then is, Will they be prepared to live a

productive life or will they be that frequent flier who ends up back in prison through the turnstile of a criminal life?

So in Texas we improved and increased programs designed to help men and women to take responsibility for their crimes and to prepare them for reentry into society. The results were pretty startling. Between 2007 and 2012, our overall rate of incarceration fell by 9.4 percent—almost 10 percent—the crime rate dropped by 16 percent, and we saved more than $2 billion worth of taxpayer money and we were able to shutter three prison facilities in the process.

I wish to return briefly to the crime rate. Former Attorney General Mukasey, a longtime Federal judge in New York, made the point that it is not the incarceration rate that measures the success of our sentencing practices, it is actually the crime rate.

I know there are many people who feel we have overincarcerated, but I think we need to keep our eye on the ball; that is, on the crime rate. As a result of these reforms in Texas, our total crime rate dropped by 16 percent, something worth paying attention to, but even more impressive than these statistics are the stories I have heard from former inmates who have actually taken advantage of this opportunity to turn around their lives. They paint a powerful picture of how these reforms can be used and the potential impact of this legislation across the country.

Again, nobody is naive enough to think everybody is going to have a turnaround story and experience like this, but last week I had the chance to visit with a number of faith-based and nonprofit groups in Houston this time, as well as some of the former inmates they have supported—all of whom are helping inmates prepare to reenter society set up for success rather than failure.

I was particularly struck by the story of one young man by the name of Emilio Parker. By the time he was 33, Emilio had spent almost half of his life in prison, including several years in solitary confinement. He started using drugs at a very early age, and after he became addicted he found more and more opportunities for crime to feed his addiction. Spending so much time in prison leaves little chance to acquire skills to succeed once you are outside, but fortunately for Emilio he found the support needed in a group called SER-Jobs for Progress in Houston. SER stands for Service Employment Redevelopment. A strange acronym, SER, but it is a community group whose mission is to equip people such as Emilio for the workforce. Their organization has helped turn around many lives in astounding ways, and Emilio was no exception.

When he started the job readiness program SER offered, he didn't know how to turn on a computer, but with their help he graduated with the program, and it helped put him on a new direction in life—one that did not include prison.

His success represents the tremendous opportunity we have before us to enact similar reforms on the Federal level in order to offer rehabilitation to inmates, reduce crime, and save taxpayers' hard-earned money.

Part of this legislation is to focus on the people most likely to take advantage of these opportunities, low- and medium-risk inmates. Indeed, what we offer them is credit, if they participate in these programs, to lesser confinement; for example, a halfway house or the like. These are the folks we believe are most likely to have learned from their experience in prison and will take advantage of the opportunity and turn around their lives. High-risk criminals who have made a life of crime I think are the least likely to take advantage of these programs and will not be available under this legislation. If it is successful, we might want to reconsider that and see whether it can be expanded.

The Sentencing Reform and Corrections Act truly represents how the Senate was meant to function: in a bipartisan manner that can effect long-lasting change for the benefit of the American people.

I thank Chairman GRASSLEY for his leadership—this would not have happened without him—and his commitment to bring us together to develop a bill that provides needed reforms to our criminal justice system. This is an extraordinary moment, where we have people on differing ends of the political spectrum coming together and finding a place where we can reach consensus.

I am particularly pleased, as I have indicated, that the CORRECTIONS Act, authored by Senator SHELDON WHITEHOUSE and me, is such a key part of this package. Pretty much everyone agrees our prisons are dangerously overcrowded and that recidivism rates—when offenders land back in prison—are too high. The hard part is coming up with a solution that addresses these problems and yet breaks the cycle of reincarceration without jeopardizing public safety. And nothing we are doing will jeopardize public safety. That should be the litmus test of anything we do. I do believe this legislation strikes that balance by building on our experience in Texas and other States across the country and focusing on rehabilitation for low-level offenders and tough sentences for hardened criminals.

I know the Presiding Officer, who was attorney general of his State of Alaska, has had a lot of experience in this area. I remember in law school one of the things we learned is that one of the goals of our criminal justice system is to rehabilitate people—to help them turn around their lives—but over the years we have almost forgotten that. I think what we have demonstrated by the Texas experience—and other experience—is that through faith-based volunteers, through job training, through helping people deal with their drug and alcohol addiction—which oftentimes exacerbates their problems and puts them behind bars, like Emilio—we can literally offer a helping hand for those who will take advantage of it. For those who are truly nonviolent and low-level offenders, this bill does represent a second chance.

This bill also reforms and improves law enforcement tools, such as mandatory minimum sentences, without eliminating them or reducing them across the board. This was a tough negotiation because, in particular, some of our Senators were focused on sentence reduction, but I have to say I have been very aware that we can't handle this on an across-the-board basis. Sentences have to be appropriate for the individual behavior and misconduct of the defendant themselves, not just some across-the-board panacea. By targeting those who are most likely to reoffend and teaching them how to succeed in the real world, we can not only reduce the crime rate—as our experience has shown in Texas—but help people turn around their lives and save billions of dollars.

So at a time when the news likes to report the divisions and polarizations here in Washington—and there are plenty of important fights, and I am not opposed to fighting for principles, but there are a lot of areas like this where we can continue to work together productively. In fact, as I said earlier, the whole system of our Constitution was designed to force consensus before big decisions such as this are made. That is the way it should be because any time a minority or even one political party can force their will on the other party—as we have seen happen before—it doesn't end well. When our system works the way it should, by people of good faith coming together, seeing a problem, trying to come up with a solution, and working together on a bipartisan basis, our system works very well. I believe this is a good example.

I look forward to working with all of our colleagues once this bill is voted out of the Judiciary Committee—which I believe it will be on Thursday—as we anticipate action here on the floor. Perhaps other Senators have other ideas that will actually improve the legislation we have crafted so far, but I do believe the President is amenable to considering a bill in this area. He has said so publicly. Again, this is another of those rare opportunities we can have to work together with the President to try to solve a problem, help save money, and help people turn around their lives.

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.

Mr. NELSON. 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. NELSON. Mr. President, I will vote for the cyber security bill. Obviously, this is a whole new era of attack on our country. On September 11, 2001, we certainly realized that the two big oceans on either side of our country that had protected us for centuries—the Atlantic and the Pacific—no longer provided that protection because we could see, in the case of 2001, an attack from within. Thus, that revised so much of our defense strategy.

Now we see the other kind of attack from within that is stealthy, insidious, and it is constant because the cyber attacks are coming to the U.S. Government as well as the U.S. industry, the business community, and U.S. citizens. The threat of cyber attack is vast and it is varied, from cyber criminals who steal personal information such as credit card and Social Security numbers, to foreign governments or state-sponsored groups that steal sensitive national security information, that steal our intellectual property, and that put at risk our economy and critical infrastructure.

I want to give one example of obtaining Social Security numbers through cyber attacks or through other means. What we found in Tampa, FL, is that street crime actually subsided because the criminals had figured that either by cyber attacks or by other means of getting Social Security numbers, they could file false income tax returns and request refunds. So with a laptop, they could do what they had done previously by breaking into and entering someone's home to steal money, and it was so much easier. And that is just one small example, but just the theft of security numbers, which they use on false income tax returns—we think that is an attack which is costing the U.S. Government, in income tax, at least $5 billion a year.

We have heard all about these attacks. Some of us in the Senate have been affected by these attacks. How many times have we heard that hackers have stolen our names, our addresses, our credit card numbers? Look what the hackers did to 40 million Target customers and 56 million Home Depot customers. They accessed checking and savings account information of 76 million J.P. Morgan Bank customers. They stole the personal information of 80 million customers of the health insurance company Anthem. Those are a few examples. Target, Home Depot, J.P. Morgan, Anthem—that is just a handful of examples. Also, remember that North Korea hacked Sony. Iran hacked the Sands Casino. China hacked the U.S. Government Office of Personnel Management. They have your information and they have my information because our information is with the Office of Personnel Management.

The attacks keep coming. We are hearing from homeland security, defense, intelligence, and private sector leaders that we have to take this threat seriously and do something about it.

I must say that it was one of the most frustrating things for this Senator, as a former member of the Senate Intelligence Committee, when we were trying to pass this very same bill 3 and 4 years ago and the business community, as represented by the U.S. Chamber of Commerce, wanted nothing to do with it because they thought it was an invasion of their privacy. Times have changed, and the hacking continues.

We see that finally we are able to get through and put together a bill on which I think we can get broad support from many different groups that are concerned about privacy and about sharing of information in the business community. This bill provides the means for the government and the private sector to share cyber threat information while taking care to protect the personal information and privacy of our people. We all face the same threat, and our adversaries use similar malware and techniques. Sharing information is critical to our overall cyber security.

What this does is it directs the Director of National Intelligence, working with other agencies and building on the information sharing that is already taking place, to put cyber threat information in the hands of the private sector to help protect businesses and individuals. It authorizes private companies to monitor and defend their networks and share with each other and the government at all levels the cyber threats and attacks—all levels of government: State, local, tribal, and Federal. This is a point of contention because these activities are strictly voluntary. That is part of the problem we had 3 and 4 years ago in trying to enact this legislation. It is strictly voluntary, limited to cyber security purposes, and subject to reasonable restrictions and privacy protections.

The bill also creates the legal certainty and incentives needed to promote further sharing of information.

So what the legislation does is it sets up a hub or a portal inside the Department of Homeland Security where cyber threat information comes in, it is scrubbed of irrelevant personal information, and then it is shared inside and outside the government quickly and efficiently because, after all, if you have a cyber attack somewhere in America that suddenly has the opportunity to explode in its application, you have to have a central point at which you can coordinate that cyber attack. That is what this portal, this hub in the Department of Homeland Security is set up to do.

This Senator feels that this bill balances the urgent need to address the threat of continued cyber attacks with privacy concerns. As the vice chair of the Intelligence Committee said yesterday, this bill is just the first step.

I am delighted that Senator FEINSTEIN just walked onto the floor of the Senate. I am quoting what the Senator said yesterday: We can and we ought to do more to improve our Nation's cyber security.

I say through the Chair to the distinguished senior Senator from California that I have shared with the Senate my frustration over the last 4 years, as a former member of the Senate Intelligence Committee, that it was so hard to get people to come together. But now, finally, even though it is voluntary, we at least have a point at which, when a cyber attack comes somewhere in America, we can centralize that, it can be scrubbed of private information, and then it can be shared in our multiplicity of levels of government and the private sector to help defend against the cyber attacks.

These cyber attacks are coming every day. They are relentless. If we don't watch out, what is going to happen has already happened to someone and it is going to be happening to innumerable American businesses. I strongly urge the Senate to pass this legislation.

Since the senior Senator from California is on the floor, I wish to take this opportunity to thank her for her perspicacity, her patience, and her stick-to-itiveness. Finally, 4 years later, it is here, and we are going to pass it this week. I thank the Senator from California.

Mr. President, I yield the floor.

The PRESIDING OFFICER. The Senator from California.

Mrs. FEINSTEIN. Mr. President, I would like to respond to what the distinguished Senator from Florida said.

Senator, you know what a pleasure it was to have you on the intelligence committee. I think you understand the time that we have spent to get this bill done, which is now about 6 years, and to take this first step, not because it is a perfect step but because it is a first step that is voluntary, with new authorities that people and companies can use if they want to, and if they don't want to, they don't have to. If they want to, it can be effective in enabling companies to share cyber security information and therefore protect themselves. I know you understand this. I am so grateful for that understanding and for your help.

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

Mrs. FEINSTEIN. I will.

Mr. NELSON. Will the Senator share her thoughts with the Senate about how the Nation's national security defense depends on us being able—we have the guns, the tanks, the airplanes, the missiles, and all of that, but there is a new type of threat against the very security of this Nation, and this legislation is a first step.

Mrs. FEINSTEIN. I can try to. I remember that in 2008 there were two significant cyber bank robberies: the Royal Bank of Scotland, I think for $8 million, and Citibank for $10 million. This was not public right away because nobody wanted it known. Then you see the more recent attacks of Aramco

being taken down, Sony, and it goes on and on. The information is not often shared publicly by companies who should be asking: This happened to our company; can you share anything that might help us handle this? That kind of thing doesn't happen because everybody is afraid of liability, and so it is very concerning.

I remember when Joe Lieberman was chairman of the homeland security committee, which had a bill. As the Senator will remember, we had the information sharing part of that bill, and we sat down with the U.S. Chamber of Commerce, I believe on three occasions, to try to work out differences, and we couldn't. The U.S. Chamber of Commerce is massive and all over the United States. It includes small businesses, medium-sized businesses, and some big businesses, and there was deep concern among its members. That took years to work out.

Finally, the Senate may be ready to take a first step, and this first step is to permit the voluntary sharing of cyber information, which, if it is stripped of private data, will be protected with liability immunity and protected because it goes through a single DHS portal and doesn't go directly to the intelligence community, which was a big concern to the private community. All of this has been worked out in order to try to come up with a basis for taking this first step.

I am sorry the Senator is no longer on our committee because my friend was really a great asset, and Florida is lucky to have my friend and colleague as their Senator.

This is just the beginning. All of the iterations on this cyber legislation have been bipartisan, so that has to say something to people. We have learned as we have done the drafting on this, and we have very good staff who are technically proficient. So they know what can work and what can't work.

I hope I have answered that question from the Senator from Florida. If I can, I will go on and make some remarks on the managers' amendment.

Yesterday Senator BURR and I spoke on this floor to describe the Cybersecurity Information Sharing Act of 2015, which is now the pending business. Senator BURR filed a managers' package on behalf of both of us, and I will quickly run through that package.

This amendment is the product of bipartisan negotiations over the past several weeks within the Intelligence Committee and with sponsors of other amendments to the bill. The managers' amendment makes several key changes to the bill to clarify authorization language, improve privacy protections, and make technical changes. It also—and I think this is of note—includes the text of 14 separate amendments. Those amendments were offered by our colleagues and I am pleased that we are able to add them to this legislation.

In sum, this amendment has two main components. It makes important changes to the bill that we announced in August to address privacy concerns about the legislation. Second, it includes several amendments authored by our colleagues that had agreement on both sides of the aisle. I will run through these amendments that will be part of the managers' package, and I do so hopefully to reassure Members that these are positive amendments.

First, it eliminates a provision on government use of cyber information on noncyber crime. The managers' amendment eliminates a provision in the committee-passed bill that would have allowed the government to use cyber information to investigate and prosecute ''serious violent felonies.'' Eliminating this provision is a very significant privacy change. We made this change because it has been a top bipartisan concern and the provision had been used by privacy groups to claim that this is a surveillance bill. As the chairman made clear on the floor yesterday, it is not. One of the reasons it is not is because it prohibits the government from using information for crimes unrelated to cyber security.

Let me be clear. The chairman said it, and I will say it today. This is not a surveillance bill. We have eliminated this provision and helped, I believe, to eliminate these concerns. So, please, let us not speak of this bill as something that it isn't.

Second, it limits the authorization to share cyber threat information to cyber security purposes. The managers' amendment limits the authorization for sharing cyber threat information provided in the bill to sharing for cyber security purposes only. This is another significant privacy change, and it has been another top bipartisan and privacy group concern.

Third, it eliminates a new FOIA exemption. The managers' amendment eliminated the creation of a new exemption in the Freedom of Information Act specific to cyber information that was in the committee-passed bill. Cyber threat indicators and defensive measures shared in accordance with the bill's procedures would still be eligible for existing FOIA exemptions, but it doesn't add new ones.

Four, it ensures that defensive measures are properly limited. The bill allows a company to take measures to defend itself, as one might expect, and the managers' amendment clarifies that the authorization to employ defensive measures does not allow an entity to gain unauthorized access to a computer network.

Five, it includes the Secretary of Homeland Security as coauthor of the government-sharing guidelines. The managers' amendment directs both the Attorney General and the Secretary of Homeland Security, rather than solely just the Attorney General, to develop policies and procedures to govern how the government quickly and appropriately shares information about cyber threats. That should be a no-brainer.

Six, it clarifies exceptions to the Department of Homeland Security's so-called portal. The managers' amendment clarifies the types of cyber information sharing that are permitted to occur outside the DHS portal created by the bill. Specifically, the bill narrows communications outside of the Department of Homeland Security portal regarding previously shared cyber threat information.

Seven, it requires procedures for notifying U.S. persons whose personal information has been shared by a Federal entity in violation of the bill. The managers' amendment adds a modified version of Wyden amendment No. 2622, which requires the government to write procedures for notifying U.S. persons whose personal information is known or determined to have been shared by the Federal Government in a manner inconsistent with this act.

Eight, it clarifies the real-time automated process for sharing through the DHS portal. Here the managers' amendment adds a modified version of the Carper amendment No. 2615, which clarifies that there may be situations under which the automated real-time process of the DHS portal may result in very limited instances of delay, modification or other action due to the controls established for the process. The clarification requires that all appropriate Federal entities agree in advance to the filters, fields or other aspects of the automated sharing system before such delays, modifications or other actions are permitted.

Senator CARPER has played a very positive role on this issue. He is the ranking member on the homeland security committee. He sat down with both Senator BURR and me earlier this year. He has proposed some very good changes, and this is one of them, which is in the managers' package.

Also, the clarification ensures that such agreed-upon delays will apply across the board uniformly to all appropriate Federal entities, including the Department of Homeland Security.

This was an important change for both Senator CARPER and Senator COONS and for the Department of Homeland Security. I am pleased we were able to reach agreement on it. Essentially, it will allow a fast real-time filter—and I understand this can be done—that will do an additional scrub of information going through that portal before the cyber information goes to other departments to take out anything that might be related to personal information, such as a driver's license number, an account, a Social Security number or whatever it may be. DHS believes they can put together the technology to be able to do that scrub in as close to real time as possible.

This should be very meaningful to the privacy community, and I really hope it is meaningful because I want to believe that their actions are not just to try to defeat this bill, but that their actions really are to make the bill better. If I am right, this is a very important addition.

Again, I thank Senator CARPER and Senator COONS, and I also thank the chairman for agreeing to put this in.

Nine, it clarifies that private entities are not required to share information with the Federal Government or another private entity. This is clear now. This amendment adds the Flake amendment No. 2580, which reinforces this bill's core voluntary nature by clarifying that private entities are not required to share information with the Federal Government or another private entity.

In other words, if you don't like the bill, you don't have to do it. So it is hard for me to understand why companies are saying they can't support the bill at this time. There is no reason not to support it because they don't have to do anything. There are companies by the hundreds, if not thousands, that want to participate in this, and this we know.

Ten, it adds a Federal cyber security enhancement title. The managers' amendment adds a modified version of another Carper amendment, which is No. 2627, the Federal Cybersecurity Enhancement Act of 2015, as a new title II of the cyber bill. The amendment seeks to improve Federal network security and authorize and enhance an existing intrusion detection and prevention system for civilian Federal networks.

Eleventh, we add a study on mobile device security. The managers' amendment adds a modified version of the Coats amendment No. 2604, which requires the Secretary of Homeland Security to carry out a study and report to Congress on the cyber security threats to mobile devices of the Federal Government.

I wish to thank Senator COATS, who is a distinguished member of the Intelligence Committee and understands this bill well, for this amendment.

Twelfth, it adds a requirement for the Secretary of State to produce an international cyber space policy strategy. The managers' amendment adds Gardner/Cardin amendment No. 2631, which requires the Secretary of State to produce a comprehensive strategy focused on United States international policy with regard to cyber space.

It is about time we do something like this. I am personally grateful to both Senators Gardner and Cardin for this amendment.

Thirteenth, the managers' amendment adds a reporting provision concerning the apprehension and prosecution of international cyber criminals. The managers' amendment adds a modified version of Kirk-Gillibrand amendment No. 2603, which requires the Secretary of State to engage in consultations with the appropriate government officials of any country in which one or more cyber criminals are physically present and to submit an annual report to appropriate congressional committees on such cyber criminals.

It is about time that we get to the point where we can begin to make public more about cyber attacks from abroad because it is venal, it is startling, it is continuing, and in its continuation, it is growing into a real monster. Let there be no doubt about that.

Fourteenth, it improves the contents of the biennial report on implementation of the bill. The managers' amendment adds a modified version of the Tester amendment No. 2632, which requires detailed reporting on, No. 1, the number of cyber threat indicators received under the DHS portal process—good, let's know—and, No. 2, the number of times information shared under this bill is used to prosecute certain cyber criminals. If we can catch them, we should. We should know when prosecutions are made. Then, No. 3 is the number of notices that were issued, if any, for a failure to remove personal information in accordance with the requirements of this bill.

Mr. President, I am spending a great deal of time on these details because there are rumors beginning to circulate that the bill does this or does that, which are not correct. This managers' package is a major effort to encapsulate what Members on both sides had concerns about. And I think the numbers of Republican and Democratic amendments that are incorporated are about equal.

Fifteenth, this managers' amendment improves the periodic sharing of cyber security best practices with a focus on small businesses. The managers' amendment adds the Shaheen amendment No. 2597, which promotes the periodic sharing of cyber security best practices that are developed in order to assist small businesses as they improve their cyber security.

I think this is an excellent amendment and Senator SHAHEEN should be commended.

Sixteenth, the managers' amendment adds a Federal cyber security workforce assessment title. The managers' amendment adds Bennet-Portman amendment No. 2558, the Federal Cybersecurity Workforce Assessment Act, as a new title III to this bill. The title addresses the need to recruit a highly qualified cyber workforce across the Federal Government.

There are just a few more, but, again, I do this to show—and the chairman is here—that we have listened to the concerns from our colleagues and we have tried to address them, so nobody should feel we are ramming through a bill and that we haven't considered the views from others. The managers' amendment is, in fact, a major change to the bill that reflects this collegial—sometimes a little more exercised, but collegial—discussion. Does the chairman agree?

Mr. BURR. Mr. President, I appreciate the opportunity to say that I totally agree. The vice chairman and I have worked aggressively for the entirety of the year where we had differences, and we found ways to bridge those differences, where we heard from Members, where we heard from associations, where we heard from businesses. We worked with them to try to accommodate their wishes, as long as it stayed within the spirit of what we were trying to accomplish, which is information sharing in a voluntary capacity.

The vice chair and I came to the floor yesterday and said if an amendment—if an initiative falls outside of that, then we will stand up and oppose it because we understand the role this legislation should play in the process.

The vice chairman said this is the first step. I don't want to scare Members, but there are some other steps. We are not sure what they are today or we would be on the floor suggesting those, but if we can't take the first step, then it is hard to figure out what the next and the next and the next are. So I am committed to continuing to work with the vice chairman and, more importantly, with all Members to incorporate their great suggestions as long as we all stay headed in the same direction, and I know the vice chairman and I are doing that.

Mrs. FEINSTEIN. Mr. President, I thank the chairman very much. If I may, through the Chair, I want the chairman to know how much I appreciate this tack he has taken to be flexible and willing throughout this process, which extends into this managers' package. So I believe—I truly believe—what we have come up with in this managers' package and what Members have contributed to it makes it a better cyber bill. I know the chairman feels the same way. We can just march on shoulder to shoulder and hopefully get this done.

I will finish up the few other items I have to discuss because I want people who have concerns to listen to what is being said because these changes have a major impact on the bill.

Next, No. 17 establishes a process by which data on cyber security risks or incidents involving emergency response information systems can be reported. The managers' amendment adds Heitkamp amendment No. 2555, which requires the Secretary of Homeland Security to establish a process by which a statewide interoperability coordinator may report data on any cyber security risk or incident involving emergency response information systems or networks. This is a process for reporting, and certainly we need to know more.

Next, No. 18 requires a report on the preparedness of the health care industry to respond to cyber security threats, and the Secretary of Health and Human Services to establish a health care industry cyber security task force. The managers' amendment adds Alexander-Murray amendment No. 2719. This is a reporting requirement to improve the cyber security posture of the health care industry.

I don't think anyone wants to have their health care data hacked into. This is deeply personal material and it should be inviolate.

The provision requires the Secretary of Health and Human Services to submit a report to Congress on the preparedness of the health care industry to respond to cyber security threats. If we really want to help protect health care information, we have to know what is going on, and that is what this amendment enables. It also requires the Secretary to establish a health care industry cyber security task force.

Next is No. 19, which requires new reports by inspectors general. The managers' amendment adds a modified version of the Hatch amendment No. 2712, which requires relevant agency inspectors general to file reports with appropriate committees on the logical access standards and controls within their agencies.

Let's know what standards and what controls they have. I think it is a very prudent request of the Senator from Utah, and I am glad we were able to include it.

Next is No. 20, which adds a requirement for the DHS Secretary to develop a strategy to protect critical infrastructure at the greatest risk of a cybersecurity attack. The managers' amendment adds the Collins amendment No. 2623, which requires DHS to identify critical infrastructure entities at the greatest risk of a catastrophic cyber security incident.

This is where we have had a number of concerns recently. The chairman's staff and my staff are working on this. Remember, this is a voluntary bill, and we do not want any language that might be interpreted to imply that this is not a voluntary bill. I know Senator COLLINS has a lot of knowledge of this area, and I believe we are going to be able to work this out.

This amendment does not convey any new authorities to the Secretary of Homeland Security to require that critical infrastructure owners and operators take action, nor does it mandate reporting to the Federal Government. Its intent, which I applaud, is for the government to have a better understanding of those critical infrastructure companies that, if hacked, could cause extremely significant damage to our Nation.

In conclusion, I would like to thank my colleagues for their thoughtful and helpful amendments. I am pleased that we have such a fulsome managers' package. I believe this managers' package strengthens our bill. It adds important clarifications, including meaningful privacy protections, it does not do operational harm, and it further improves the strong bill that the Intelligence Committee passed by a strong vote of 14 to 1 earlier this year.

I wanted to do this so that all Members know what is in the managers' package, and both the chairman and I believe that these additions are in the best interests of making a good bill even better.

I thank the Presiding Officer, and I yield the floor.

The PRESIDING OFFICER (Mr. SASSE). The Senator from Alaska.

Mr. SULLIVAN. Mr. President, I wish to acknowledge the remarks of the distinguished Senator from California and the Senator from North Carolina, and I thank them for their important work on the cyber bill. I know we are going to be discussing a lot of that, and why it is important to our national security.

NATIONAL DEFENSE AUTHORIZATION ACT

This afternoon I wish to talk about another important bill that is moving its way through the process of becoming law, and that is the National Defense Authorization Act, the NDAA.

As did many of my colleagues, I spent last week back home in my great State of Alaska. In Alaska, it is hard not to see the strength and pride in our military everywhere, every day, everywhere we go. I will provide a few examples.

We have what is called the Alaska Federation of Natives Convention, an annual convention that we have with a very important group of Alaskans. The theme this year was ''Heroes Among Us'' at the convention. It was about heroes among us because Alaskan Natives serve in the U.S. military at higher rates than any other ethnic group in the country—a real special kind of patriotism. I had the honor, really, to meet dozens of these great veterans from all kinds of wars. I met veterans from World War II, the Attu campaign. A lot of Americans don't realize that Alaska was actually invaded by the Japanese and we had to fight to eject them from the Aleutian Islands. I met veterans from the Philippines campaign under General MacArthur. I met veterans from the Korean war who served at the Chosin Reservoir. I had a great opportunity to meet an Honor Flight coming back from Washington, our veterans from World War II, Korea. Of course, just walking around Anchorage you see and hear military members training all the time. We have a great base, JBER, with F–22s ripping through the sky, our military members keeping us safe. That sound is what we call in Alaska the sound of freedom, when you hear those jets roaring. It is everywhere.

In Alaska, we love our veterans and our military. We honor them. We know that providing for the national defense of our great nation, taking care of our troops, and taking care of our veterans is certainly one of the most important things we do in the Senate. Of course, it is not just Alaska. I am sure when the Presiding Officer was home in the great State of Nebraska there was the same patriotic feeling of supporting our troops and the importance of our national defense.

For the most part, that feeling exists here in Washington. I have been honored to sit on two committees that focus on these issues a lot: on the Armed Services Committee and Veterans' Affairs Committee. These are very bipartisan committees and where support for our national defense, our troops, and our veterans is across the board on both sides of the aisle—no doubt about it. But I do say ''for the most part'' because, as the Presiding Officer knows, nothing is truly as it seems in Washington, DC.

I have spoken on the floor, as a number of Senators have, about what motivated a number of us last year to actually throw our hat in the ring and run for the U.S. Senate. Like the Presiding Officer, I know a lot of us were concerned about the country going in the wrong direction, about a dysfunction in Washington, about a government that has run up an $18 trillion debt, no economic growth, our credit rating being downgraded, no amendments being brought to the Senate floor, no budget for the Federal Government attempted, no appropriations bills attempted for years. The most deliberative body in the world was certainly a body that had been shut down, and a lot of us saw a need to change that.

So we are starting to change that. We are back to regular order. We are talking about debating bills. There have been dozens, if not hundreds, of amendments already this year—last year there were only 14 amendments—and we passed a budget. We passed 12 appropriations bills to fund the government—very bipartisan—and we are focusing on the issues, whether it is cyber security, defense or taking care of our veterans, something the vast majority of the American people want us to focus on.

For example, we brought to the floor two critical appropriations bills just a couple of months ago—the Defense appropriations bill and the Military Construction and Veterans Affairs bill. These passed out of the Appropriations Committee by huge bipartisan majorities, 27 to 3 on the Defense appropriations bill and 21 to 9 on the Military Construction and Veterans Affairs bill. This is what the American people want us to do—get back to regular order, fund the government, and put together a budget. So far, so good. That is what we are called to do.

Here is where the dysfunction of Washington, DC, began to rear its head again: These bills that are critical to our troops, our defense, and our veterans—all with strong bipartisan support in committee—were brought to the floor of the Senate and they were filibustered. They were filibustered. The bill to fund our military, that funds our national defense and takes care of our veterans was filibustered—blocked—stopped by our friends on the other side of the aisle. I am not sure why. I still don't know why. As a matter of fact, I haven't seen anyone who actually voted to filibuster these important bills come down to the Senate floor and say: Here is why we voted against funding our troops. Here is why we voted against funding our veterans.

I think the overwhelming majority of Americans, regardless of what State they live in, would say: No, no, no. You need to vote for these bills that are funding our military, veterans, and national defense. That is one of the most

important things we want you to do. The bottom line on those votes is that our troops, our veterans, and our national defense were shortchanged because they didn't get funded.

Let me move on to the Defense authorization bill, what I want to talk about today. This is an annual undertaking that sets the policies, programs, and defense strategy for our military. It also authorizes spending on national defense and our military. Again, it is certainly one of the most important tasks this body does, and I think most Senators on both sides of the aisle would agree with that.

Once again, as with the appropriations bill, we were working closely together on a bipartisan basis. I was on the Armed Services Committee and this moved through the committee and it was very bipartisan. It was voted out on a strong bipartisan vote to come to the floor. I commend Chairman MCCAIN, who did a great job on that as the chairman of the Armed Services Committee, and Ranking Member REED of Rhode Island did a fantastic job. I must admit that this Senator feared a little bit of a replay in terms of the scenario we saw with the appropriations bill—meaning strong bipartisan support out of the committee and then coming to the Senate floor and being filibustered. I feared this, in part, because at one point during the Defense authorization debate the minority leader came and stated that the Defense authorization bill was ''a waste of time.''

A waste of time? Tell that to the marines, the soldiers, the airmen, the sailors, and their families—those members of the military who are defending our country right now—that this bill was a waste of time. I guarantee they would not agree with that statement. Fortunately, neither did the Senate. To the contrary, the Senate has now voted on the Defense authorization bill twice, once as an original bill and once as part of a conference report with very strong bipartisan and veto-proof majorities, with 71 Senators the first time around and 73 when we voted on it a couple of weeks ago. I mention the phrase ''veto-proof majority'' because incredibly the President of the United States, the Commander in Chief, has said he is going to veto this bill when it comes to his desk. It was just sent to him yesterday.

I don't know how the Commander in Chief is going to explain that to the troops or to their families or to the American people or to the 73 Senators who voted for that bill. It is important to recognize that although we may think this is all inside Washington and no one is really following it, something like this impacts morale when the Commander in Chief is saying: Hey, troops, I am going to veto this.

This is a copy of the Marine Corps Times. I subscribe and read the Marine Corps Times. A lot of marines and members of the military read this all over the world. Guaranteed, our men and women deployed overseas read the Marine Corps Times. In this edition there is an article about how President Obama has vowed to veto the Defense authorization bill. We have marines fighting overseas who are reading this, and they are not getting it.

This week in the Marine Corps Times:

> The MOAA [Military Officers Association of America] and other military advocacy groups have argued against the presidential veto, calling the legislation a critical policy measure that cannot be delayed. The measure has been signed into law in each of the last 53 years, and includes a host of other specialty pay and bonus reauthorizations.

In a statement from MOAA officials in this article that thousands of our Active-Duty troops are reading:

> The fact is that we are still a nation at war, and this legislation is vital to fulfilling wartime requirements. There comes a time when this year's legislative business must be completed, and remaining disagreements left to be addressed next year.

To govern is to choose. To govern is to prioritize.

President Obama's administration has spent years negotiating the Iran deal and this body spent weeks debating the President's Iran deal. We put a lot of time into it, and the President's administration put an enormous amount of time into it.

On the Iran deal, part of the hope from Secretary Kerry, the President, and others was that once it got passed by the U.S. Congress—by the way, on a partisan minority vote—that Iran would somehow start to change its behavior and say: Look, America is someone we want to partner with.

Since the Senate passed the Iran deal, let's see what has happened. Iran has sent troops to Syria. Iran has backed Hamas, which is now engaging in knife-murdering attacks against Israelis. The Iranian leader has stated that Israel shouldn't exist within the next 25 years. Iran has violated the U.N. Security Council ballistic missile resolutions, and this Senator and many others think Iran has already violated the deal by firing ballistic missiles with a range of 1,000 miles. Iran has sentenced an American reporter for the Washington Post for spying. I don't think the behavior that a lot of the supporters for this deal anticipated is happening.

More broadly, I think it is important to put into context what is going on with our national security, the NDAA, the moving forward with the Iran deal, and the President's threat to veto the NDAA. The President's Iran deal, once implemented, will be giving tens of billions of dollars to Iran, the world's biggest state sponsor of terrorism—but the President threatens to veto the Defense bill that actually funds our military. The President's Iran deal will lift sanctions on Iranian leaders such as General Soleimani, who literally has the blood of American soldiers on his hands—but the President threatens to veto U.S. troop pay bonuses and improved military retirement benefits. The President's Iran deal gives Iran access to conventional weapons, ballistic missile technology, and advanced nuclear centrifuges—but the President threatens to veto funding for advanced weapons systems for our Armed Forces. Finally, the President's Iran deal certainly is going to allow more funding for terrorist groups like Hezbollah and Hamas—but the President is threatening to veto a bill that provides additional resources for our troops to fight terrorists such as ISIS.

To govern is to choose. To govern is to prioritize. Has it really come to the point where the White House is more focused on freeing up funds for Iranian terrorists than funding America's brave men and women in uniform? I certainly hope not.

I ask all of my fellow Senators who voted for this bill in a very strong bipartisan way and my fellow Alaskans and Americans to reach out to the White House. Let them know that you oppose the President's veto of this bill.

What we need is a strong military, particularly now. We need to support our troops and our veterans, and we need President Obama to sign—not veto—this bill which is critical to our national defense.

I yield the floor.

The PRESIDING OFFICER. The Senator from Maryland.

Mr. CARDIN. Mr. President, I ask unanimous consent to speak as in morning business.

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

43RD ANNIVERSARY OF THE CLEAN WATER ACT AND EPA'S CLEAN WATER RULE

Mr. CARDIN. Mr. President, this past Sunday was the 43rd anniversary of the enactment of the Clean Water Act. In 1972, the Clean Water Act amended the Federal Water Pollution Control Act, which was the first major U.S. law to address water pollution. This law was enacted with bipartisan support—I could really say on a nonpartisan issue—because the Congress in 1972 and the administration recognized that clean water was in our national interest. It was important to our public health, it was important to our environment, and it was important to our economy. This law established the basic structure for regulating pollutant discharges into the waters of the United States, and it has been the cornerstone of our efforts to protect our Nation's waterways.

Several times we have done cost analysis of the cost of regulation versus the benefit of clean water. It is overwhelmingly on the side of the benefit to our community, better health, better environment, and a better economy. On this occasion I would like to speak about the recent efforts to protect America's waterways, such as the EPA's final clean water rule, and why we should defend these efforts and allow nationwide implementation.

In May, the EPA released their final clean water rule, which completed another chapter in the Clean Water Act's

history. As the Clean Water Act worked to restore the health of our Nation's water resources, we saw the U.S. economy grow, demonstrating that America does not have to choose between the environment and a robust economy. A clean environment helped build a robust economy.

Two Supreme Court decisions, however, call on the EPA and the Army Corps to clarify the definitions of the waters of the United States. The EPA's final rule restores some long overdue regulatory certainty to the Clean Water Act. I might tell you, in reviewing this rule, it basically reestablishes the longstanding understanding of what were the waters of the United States and what was subject to regulation.

This rule allows the Clean Water Act to continue its important function of restoring the health of our Nation's waters. The rule became effective this August, but immediately following the implementation and on this anniversary, there have been unprecedented attacks on the final rule. As the rule came out, a Federal district court in North Dakota granted a preliminary injunction, blocking its implementation.

The EPA continued to implement the rule in all States but the 13 States that filed the suit that led to the injunction. However, in October, the U.S. Court of Appeals for the Sixth Circuit decided to stay the implementation of the rule for the entire country. This attempt to overturn the clean water rule is dangerous, shortsighted, and a step away from good governance, public health, and commonsense environmental protection.

Let me tell you what is at risk. What is at risk are our Nation's streams and 200 million acres of wetlands. Over half of our streams and over 200 million acres of wetland are now at risk of not being under regulation under the Clean Water Act.

These protections are needed for drinking supplies for one out of every three Americans. I am very concerned about the impact on all States, but let me just talk for a moment, if I might, about my own State of Maryland. Marylanders rely upon our water as part of our life. We live on the water. Seventy percent of Marylanders live in coastal areas. We depend upon clean water. We are particularly concerned about our drinking supply of water as well as the health of the Chesapeake Bay.

We are at risk with the waters of the United States confusion out there because of the Supreme Court decisions and now the stay of this rule by the court. The Clean Water Act and EPA's final rules are essential to the health of the Chesapeake Bay. Wetland protections are especially critical to the Chesapeake Bay because the wetlands soak up harmful nutrient pollution.

This past Monday, I was in Howard County at a NOAA announcement of the Chesapeake Bay B-WET grant. These are bay, watershed, education, and training funds. These are small dollars that go to institutions to help educate our children. In this case, the Howard County Conservancy received a grant because they bring all of the students from the Howard County public schools to an outdoor experience to rate and judge the streams in our community.

The streams, of course, flow into the Chesapeake Bay. They are giving us a report card. I must tell you, that report card is not going to be as good as it should be. Without the protections in the Clean Water Act, it is going to be more difficult to meet the goals we need to in order to protect the Chesapeake Bay and all of the watersheds in this country for future generations.

The health of the bay is closely linked to upstream water quality and the restoration and protection of headwaters. It should go without saying that these waters are located in States beyond Maryland's borders. Improvements to upstream water quality are positively correlated with the water quality of the bay. We need a national program. That is what the Clean Water Act is. It is a national commitment because we know that the watersheds go beyond State borders.

In Maryland, we set up the Chesapeake Bay Partnership. Yes, Virginia and Maryland are working together, but we also have the cooperation of Pennsylvania, of New York, of West Virginia, of Delaware. Why? Because these States contribute to the water supplies going into the Chesapeake Bay. We need to protect these waters.

Protecting of America's waters is critically important to public health. So what is at stake here? What is at stake if we derail the clean water rule? The public health of the people of Maryland and all States around this country. Public health and the environment in my State and the States of my colleagues have become seriously at risk from this decision that hinders this essential commonsense guidance.

I hope the court moves swiftly to affirm the rule in its final decision and restores the invaluable protections needed for the drinking supplies of one out of every three Americans. As we recognize the anniversary of the Clean Water Act, I want us to continue to defend this Nation's waters from pollution. This act ensures that every citizen receives the clean water they need and deserve.

The EPA's final clean water rule provides further regulatory clarity that we need to ensure the health of our water resources. I urge my colleagues to continue to defend and fight for clean water as we recognize the 43rd anniversary of the Clean Water Act. Every Congress should, as its legacy, add to the protections that we provide for clean water in this country. That should be the legacy of every Congress, but we certainly don't want to hinder that record. Therefore, we need to implement the EPA's clean water rule nationwide. I urge my colleagues to support such action.

I yield the floor.

The PRESIDING OFFICER. The Senator from California.

AMENDMENT NO. 2612, AS MODIFIED

Mrs. FEINSTEIN. Mr. President, I call for the regular order with respect to the Franken amendment No. 2612.

The PRESIDING OFFICER. The amendment is now pending.

AMENDMENT NO. 2612, AS FURTHER MODIFIED

Mrs. FEINSTEIN. Mr. President, I ask that the amendment be further modified to correct the instruction line in the amendment.

The PRESIDING OFFICER. The amendment is so further modified.

The amendment, as further modified, is as follows:

Beginning on page 4, strike line 9 and all that follows through page 5, line 21, and insert the following:

system that is reasonably likely to result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

(B) EXCLUSION.—The term ''cybersecurity threat'' does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(6) CYBER THREAT INDICATOR.—The term ''cyber threat indicator'' means information that is necessary to describe or identify—

(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

(B) a method of defeating a security control or exploitation of a security vulnerability;

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(E) malicious cyber command and control;

(F) the harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

(G) any other attribute of a cybersecurity threat, if disclosure of such information is not otherwise prohibited by law; or

Mrs. FEINSTEIN. Thank you.

The PRESIDING OFFICER. The Senator from North Carolina.

AMENDMENT NO. 2581, AS MODIFIED

Mr. BURR. Mr. President, I call for the regular order with respect to the Cotton amendment No. 2581.

The PRESIDING OFFICER. The amendment is now pending.

The Senator from Louisiana.

MENTAL HEALTH REFORM ACT

Mr. CASSIDY. Mr. President, for 25 years I have worked in the Louisiana public hospital system. You cannot help but notice when you work in a public hospital system, but also in private hospitals, how often mental health issues are directly a part of a

patient who comes to see you. It does not just have to be a physician seeing patients in the emergency room. Each of our families, mine included, has a family member or a friend with serious mental illness. It is nonpartisan. It cuts across demographic lines.

If I go before a group anywhere in my State, indeed anywhere in the Nation, and bring up the need to address serious mental illness, all heads nod yes. It is true of my family. It is true of yours. It is true of almost everybody watching today. I am old enough to remember when people would not speak of cancer. There was a stigma associated with having cancer. That is long gone, much to our advantage, but for some reason, there continues to be a stigma, a shame, associated with mental illness. I will argue that stigma and sense of shame has retarded what we can do.

This is something that we have to address, we have to discuss, and we have to go forward. The discussion right now, frankly, is being driven by tragedy: Lafayette, Louisiana; Newtown; Charleston; Oregon; Tennessee. We have heard stories and they are beyond heartbreaking, but what is not spoken of are the broken families, the parents that know there is something wrong with their child but do not know where to go to receive help, ending up in an overcrowded emergency room or with their child in a jail or prison when a more appropriate setting would be elsewhere.

It is in the midst of these terrible tragedies that at least we can hope they can serve as a catalyst for society and Congress to begin to fix America's broken mental health system. Maybe something good can happen, even from tragedies as horrific as these.

The question is, If one of the roles of Congress is to respond to societal needs that justify Federal involvement, should we not ask ourselves why has there been such a failure to address the issue of serious mental illness? I am pleased to say that my colleague, Senator CHRIS MURPHY, and I wish to change that. We have introduced the bipartisan Mental Health Reform Act, which now has 10 cosponsors, both Republican and Democrat.

Our bill begins to fix our mental health system and attempts to address the root cause of mass violence, which is recognized but untreated mental illness. How does our bill begin to do so? First, patients too often cannot get the care they need and too often have a long delay between diagnosis and treatment. Access delayed is access denied. Access is hampered by a shortage of mental health providers and too few beds for those with serious mental illness who truly need to be hospitalized.

Related to this, right now people with major mental illness tend to die from physical illness as much as 20 years younger than someone who does not have serious mental illness. As a physician, I know if we treat the whole patient, if we integrate care, it is better. Medicaid, though, by policy, will not pay for a patient to see two physicians on the same day.

So imagine this: A family practitioner sees a patient who clearly has major mental illness and, because the patient is right there, would like him to walk down the hallway to see her friend the psychiatrist, to have both addressed immediately while the patient is there. Medicaid will not pay the psychiatrist. On the other hand, the patient might be seeing a psychiatrist and have seriously high blood pressure or evidence for diabetes out of control, but the psychiatrist cannot say: Wait a second. Let me walk you down the hallway to see my colleague, the family practitioner, because Medicaid will not pay for that. By the way, private health insurance will. This is a policy change we need for public health insurance. Our bill would allow patients to use both mental and physical health services the same day.

Secondly, most people have their first episode of serious mental illness between the ages of 15 and 25, starting down a path that ends with their life and their family's lives tragically altered. This bill attempts to identify those young folks, stopping that path from ever opening up, and preventing the first episode of serious mental illness or, if it does occur, leading them on a path of wholeness, a path towards wellness.

Another thing our bill does is it establishes a grant program focused on intensive early intervention for children who demonstrate those first signs that can evolve into serious mental illness that may only occur in adolescence or adulthood. A second grant program supports pediatricians who are consulting with mental health teams. This program has already been successful in States such as Massachusetts and Connecticut.

Third, without appropriate treatment options, prisons, jails, and emergency rooms have become the de facto mental health care providers. More than three times as many mentally ill are housed in prisons and jails than in hospitals, according to the National Sheriffs' Association. Overcrowded U.S. emergency rooms have become the treatment source of last resort for psychiatric patients. We incentivize States to create alternatives where patients may be seen, treated, and supervised in outpatient settings, as opposed to being incarcerated.

Our bill creates an Under Secretary for Mental Health within the U.S. Department of Health and Human Services. This Under Secretary's responsibility would be to coordinate mental health services across the Federal system to help identify and implement effective and promising models of care.

It reauthorizes successful programs, such as the community mental health block grant and State-based data collection. The bill also increases funding for critical biomedical research on mental health. On top of this, it strengthens the transparency and enforcement of mental health parity by requiring the U.S. Departments of Labor, Health and Human Services, and Treasury to audit the implementation of the mental health parity movement to determine the parity between mental and physical health services.

Our bill does other things, but the most important thing it does is it helps prevent tragedies. It helps families, and it helps those broken individuals affected by mental illness become whole.

In 2006, William Bruce of Maine was a 24-year-old who needed help. He suffered with schizophrenia and had been hospitalized. Without contacting his parents, our broken health care system allowed William to be released—even though his doctors said he was ''very dangerous indeed for release to the community.'' Sadly, 2 months later he murdered his mother at home with a hatchet. This story is tragic and heartbreaking, and even worse, it could possibly have been prevented if we had worked then to fix our broken mental health system. We wish to fix it now so there is not another such episode in the future.

The time for mental health reform is now. If not now, when? If not us, who? If not now and not us, there will be more Lafayettes, Newtowns, Charlestons, Tennessees, Oregons, and more broken families.

This bill does not wave a magic wand, but it puts us on a path where we can say these things that once occurred perhaps no longer will.

Thank you.

I yield back the remainder of my time.

The PRESIDING OFFICER (Mr. PERDUE). The Senator from Connecticut.

Mr. MURPHY. Mr. President, I am on the floor today to join my good friend from Louisiana, Senator CASSIDY, as we formally introduce to the Chamber the Mental Health Reform Act of 2015. I thank him personally for all the time he has put into this not only as a Member of the Senate but previous to this as a Member of the House of Representatives.

This effort is patterned after a bill Senator CASSIDY and my namesake, Representative TIM MURPHY of Pennsylvania, worked on for years in the House of Representatives.

I wish to begin by sharing a story with you—that is the way Senator CASSIDY ended. I will talk about a woman from Bloomfield, CT, named Betsy. She has a 28-year-old son, John, who suffers from schizoaffective disorder. It is a serious mental illness whose signs began showing when John was 15 years old. He was hospitalized—think about this—15 different times between the ages of 15 years old and 18 years old, generally only for time-limited stays ranging from about 5 days to maybe 2 weeks. Despite the severity of the condition, he was told upon discharge there was really nowhere for him to go, no permanent solution for this young

man. He was just an adolescent, but his parents were told there was no place for him to be treated. What resulted was not only John getting to a breaking point but his parents as well.

As we know, serious mental illness doesn't affect just the individual person, it also affects family members who are trying to care for them.

Without needed supports and services, John became increasingly remote and psychotic until he was hospitalized again. Upon discharge this time, John went to a shelter—the only place he could go. Since he couldn't follow the shelter's rules, John, whom his mother said was ''young, fragile, vulnerable and mentally unstable,'' was kicked out to survive homeless on the streets.

John finally—finally—was able to get a bed at a place that was able to house him for longer than 2 weeks, Connecticut Valley Hospital. That ability to get John stabilized for a longer period of time, get him into a real treatment plan, allowed him to then transfer into a community bed in Middletown, CT. That is where John is today. John has been living successfully out in the community for 3 years. But we spent millions of dollars on John's care, which led to no better outcome for him. We wasted millions of dollars and potentially thousands of hours of time because he was shuttled in and out of hospitals without any long-term treatment and without any hope for him and his family.

What Senator CASSIDY and I are trying to say is that there is a better way. We are already spending billions of dollars on inadequate mental health care in this country. We need to do better, but a lot of this is just about spending money in a more effective way.

One of the programs our bill helps fund is an early-intervention program for individuals who show their first episode of psychosis. The program the National Institutes of Mental Health just evaluated—with findings released yesterday—was the RAISE Program. And in Connecticut we run a similar program called the STEP Program. What this study showed yesterday is that if you provide wraparound services to an individual who shows a first episode of psychosis—comprehensive, immediate services—you can get a dramatic decrease in the number of episodes they show later in life. In Connecticut, we found that the STEP Program reduced hospitalizations by nearly 50 percent after individuals were given those wraparound services immediately. When they did need hospitalizations later on, they were on average 6 days less than when you didn't provide those wraparound services.

These are the types of programs that could have helped Betsy's son John early so that he could have started his recovery as a teenager rather than in his twenties. They could have saved the U.S. Government and the State of Connecticut a lot of money as well.

The trendlines beyond the anecdotes are very disturbing. Mental illness has been on the rise for the past few decades. One out of five adults today is coping with mental illness. If you look at the time period from 1987 to 2007, the number of people with mental disorders who qualify for SSI has risen by 2½ times. From 1980 to 2000, we put up to 72,000 people in our jails who prior to deinstitutionalization would have been in psychiatric hospitals—people who are in jail primarily or only because of their psychiatric disorder.

Just in the last 2 years alone, the number of people that HRSA estimates to be living in a mental health shortage area has gone from 91 million—that is pretty bad to start with—up to 97 million. That is just 2 years of data. Since 2005, we have closed 14 percent of our inpatient beds in this country. So what is happening is a dramatic increase in the number of people who are suffering from mental illness and a rather dramatic decrease in both outpatient and inpatient capacity. We have to provide more resources to meet the demand, but we also have to spend money better.

Senator CASSIDY covered our piece of legislation accurately, so I won't go into detail, but I wish to talk about our process. What we decided to do at the beginning of this year was bring together all of the groups—the provider groups, the advocacy groups, the hospital groups—who have worked on this issue for years and then bring in those in the House of Representatives who have been working on this as well: Representative TIM MURPHY and EDDIE BERNICE JOHNSON.

They have a bipartisan reform bill in the House. We decided not to start from scratch but to take their piece of legislation, knowing that it has a good chance of passage in the House, and try to build on it and improve it.

We spent 6 months meeting with all of these groups and coming up with our own consensus product that today has the support of a cross-section of behavioral advocacy groups all across the country, including the National Alliance for the Mentally Ill, the National Council for Behavioral Health, the American Psychological Association, the American Psychiatric Association, social workers, the American Foundation for Suicide Prevention, and the list goes on. We also went out to our colleagues as well, knowing that nothing in the Senate can pass without not just bipartisan support but bipartisan support that reflects the diversity of both of our caucuses. We think we were able to build a good foundation of cosponsors for this bill: Senators FRANKEN, STABENOW, BLUMENTHAL, and SCHUMER on the Democratic side, and Senators MURKOWSKI, COLLINS, VITTER, and CAPITO on the Republican side. We hope that this coalition of groups on the outside, this alliance with a reform effort in the House that we believe has legislative legs, and a good one-for-one with some cosponsors in the Senate, will allow us to move this bill forward, and we have to. We have to.

So I will end where Senator CASSIDY began his remarks, which is why the Nation's attention has turned to this question of how we reform our mental health system. We lived through a tragic and gut-wrenching episode of mass destruction in Newtown, CT. Senator CASSIDY has had his own experience with mass tragedy. The reality is that the reasons why we see these episodes of mass shootings are complicated, but if you read the report on Adam Lanza's intersection with Connecticut's mental health system, you will see that it failed him. It failed him and it failed his family. I don't know that correcting the mental health system alone would have changed what happened in Newtown, but I know that if we fix our mental health system, we will have a downward pressure on the episodes of mass violence that happen in this country.

But, as Senator CASSIDY said, we should fix our mental health system because it is broken for everyone, regardless of whether an individual has a predisposition towards violence, because, of course, the reality is that people with mental illness are much more likely to be the victims of violence than they are to be the perpetrators of violence. So there is no inherent connection between mental illness and violence. But these mass shootings have drawn the Nation's attention to what Congress can agree on right now that will try to improve public safety across this Nation.

We are not going to get a background checks bill this year. I hoped we could, but we won't. What we can get is a mental health reform bill, and that will help everyone—the case in Maine, the individual in Bloomfield, and millions of others who have had a miserable experience with a mental health system that is broken today, in part because of lack of coordination and in part because of lack of funding.

I am so thankful to Senator CASSIDY for being with me on the floor today. I am grateful for his friendship and for his cooperation on bringing this truly bipartisan Mental Health Reform Act to the floor of the Senate. We recommend it to our colleagues. We look forward to the upcoming hearings in the HELP Committee that we both sit on, and we hope to be back on the floor of the Senate as soon as possible to move forward on its passage through this body.

I say thank you to my colleague in the Senate, Senator CASSIDY.

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.

Mr. GRASSLEY. 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. GRASSLEY. Mr. President, I rise to express my strong support for the

bill before the Senate, S. 754, the Cybersecurity Information Sharing Act, and I want to thank the bill's managers for their leadership in drafting this bill and putting a lot of hard work into the bill.

Cyber security challenges that threaten us are very real challenges. We receive almost daily reminders of the importance of effective cyber security to protect our private data and the safety and security of the entire Nation from cyber attacks. These attacks have compromised the personal information of so many Americans as well as sensitive national security information. That national security issue might even be the biggest of the ones we hope to deal with.

The legislation before us will encourage the government and the private sector to work together to address these cyber security challenges. This bill helps create a strong legal framework for information sharing that will help us respond to these threats. The bill authorizes private companies to voluntarily share cyber threat information with each other and with the government. In turn, the bill permits the government to share this type of information with private entities.

The bill reduces the uncertainty and, most importantly, the legal barriers that either limit or prohibit the sharing of cyber threat information today. At the same time, the bill includes very significant privacy protections to strike a balance between maintaining security and protecting our civil liberties. For example, it restricts the government from acquiring or using cyber threat information except for limited cyber security purposes.

So, as I did at the beginning, I want to salute the leadership of the chair and vice chair of the Select Committee on Intelligence, Senator BURR and Senator FEINSTEIN, for their efforts on this bill. I know from the last couple of Congresses that this type of legislation isn't easy to put together. In the 112th Congress, I cosponsored cyber security legislation along with several of my colleagues. This involved working across several committees of jurisdiction. Last Congress, as then-ranking member of the Judiciary Committee, I continued to work with the Select Committee on Intelligence and others on an earlier version of this bill. Unfortunately, Democratic leadership never gave the Senate an opportunity to debate and to vote on that bill in the last Congress.

Senators BURR and FEINSTEIN were undaunted, however, and this Congress they diligently worked and continued to seek input from relevant committees of jurisdiction, including the Judiciary Committee that I chair. They incorporated the views of a broad range of Senators and worked to address the concerns of stakeholders outside of the Congress. This has produced their managers' amendment.

This is a bill that enjoys broad bipartisan support. As with most pieces of legislation that come before the Senate, it is not a perfect piece of legislation from any individual Senator's point of view, but in finding common ground, it has turned out to be a good bill that addresses a very real problem.

It is time for us to do our job and to vote. This is how the Senate is supposed to work. Now is the time for action because the question isn't whether there will be another cyber attack, the question is when that attack will happen.

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.

Mr. BURR. 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. BURR. Mr. President, I am here to briefly talk on S. 754, the cyber security bill. Yesterday Vice Chairman DIANNE FEINSTEIN and I came to the floor and encouraged our Members who had amendments or who had an interest in debating the bill to come to the floor. It was my hope that we could finish in a couple of days with the cooperation of Members. We have not gotten that level of cooperation. Therefore, this will take several more days to finish. But it doesn't lessen the importance for those Members who have amendments in the queue—meaning they are pending—to come to the floor and talk about their amendments if they would like to. At some point, we will culminate this process, and those amendments that have yet to be disposed of will have votes with a very limited amount of debate time included.

It is my hope that we will have a wholesome debate and that people will have an opportunity to know what is in this bill if they don't today. But more importantly, through that debate we are able to share with the American people why a cyber security bill is so important and, more importantly, why we have done it in a way that we think it will be embraced and endorsed by not just corporate America but by individuals throughout the country.

Let me announce today that this bill will be done either Monday evening or Tuesday morning based upon what the leadership on both sides can agree to as it relates to the debate. The Vice Chair and I also came to the floor and we made this statement: We have worked aggressively in a bipartisan way to incorporate in the managers' package, which is currently pending, 14 amendments, and 8 of those amendments were included in the unanimous consent agreement made earlier this year when we delayed consideration of the bill until the day when we moved forward. There were several amendments on which we weren't able to reach an agreement or that we believed changed the policy significantly enough that this was not just an information sharing bill that was voluntary for corporations throughout this country. In the absence of being able to keep this bill intact in a way that we thought we needed to, the Vice Chairman and I have agreed to lock arms and to be opposed to those additional amendments.

Having said that, the debate to date has focused on the fact that there are technology companies across this country that are opposed to this bill. Yesterday the Vice Chairman and I repeatedly reminded our colleagues and the American people that this is a voluntary bill. There is nothing mandatory in it. The reality is that if you don't like what is in this, if for some reason you don't want to participate in what I would refer to as a community watch program—it is real simple; it is voluntary—do not participate. Choose not to inform the Federal Government when hackers have penetrated your system and stolen personal data out of it. Just choose not to tell us. But do not ruin it for everybody else. In a minute I am going to go through again why I think the cyber security bill should become law, why I think this is the first step of how we protect the personal data of the American people, and why hundreds, if not thousands, of businesses support this information sharing bill. But I can't stress that enough for those who oppose this. Most of them are, in fact, companies that hold the most private data in the world. Let me say that again. Those who are expressing opposition to this bill hold the largest banks of personal data in the world.

The decision as to whether they are for the bill or against the bill is their decision. The decision whether they utilize this voluntary program to further protect the personal data that is in their system is between them and their customers. But I have to say that it defies reason as to why a company that holds that much personal data wouldn't at least like to have the option of being able to partner with the Federal Government in an effort to minimize data loss, whether it is at their company or whether it is in their industry sector or whether it is in the global economy as a whole.

The last time I checked, the health of U.S. businesses was reliant on the health of the U.S. economy, and the health of the U.S. economy is affected by the health of the global economy. I know the Presiding Officer understands that because he was in business like I was for 17 years.

It really does concern me that one could be opposed to something that insulates the U.S. economy from having an adverse impact by the cyber security act and believes that they are OK even though it might tank the U.S. economy.

At the end of the day, I want to try to put this in 101 terms, the simplest terms of what the information sharing bill does. I am going to break it into three baskets. It is about business to

business. This bill allows a company that has been hacked—where somebody has penetrated their computer system and has access to their data—to immediately pick up the phone and call their competitor and ask their competitor whether they have had a similar penetration of their system.

It is only reasonable to expect that the first person you would go to is a company that has a business that looks exactly like yours. In that particular case, this legislation provides that company with protection under the anti-trust laws. Anti-trust forbids companies from collaborating together. What we say is that if it has do with minimizing the loss of data, we want to allow the collaboration of competitors for the specific reason of discussing a cyber attack.

The Senate recognizes I have designed something in this that doesn't require a corporate lawyer to sit in the room when the decision is made. I have no personal dislike for lawyers other than the fact that they slow things down. To minimize the loss of data means you have to have a process that goes in real time from the bottom of the chain all the way to the decision-making and the communication back down, not only to that business, but to the entire economy. Having a lawyer that has to think whether we can legally do this defeats the purpose of trying to minimize data loss. So we give them a blanket exemption under the anti-trust laws so they know up front that they can pick up the phone and call their competitor, and there is no Justice Department that will come down on them as long as they confine it to the discussion of cyber attack.

At the same time we initiate what I call business to government, which means that when the IT department is talking to their competitor, the IT department can put out a notification through the Federal portal that they have been attacked, and that initiates the exchange of a limited amount of information that has been predetermined by everybody in the Federal Government who needs to do the forensics of who attacked, what tool they used, and what defensive mechanism could be put up in the way of software that would eliminate the breach.

In the statute we have said, one, you can't transmit personal data unless it is absolutely crucial to understanding the forensics of the attack. We have also said in statutory language to the government agencies: If for some reason personal data makes it through your filters, you cannot transmit that personal data anywhere else within the Federal Government or to the public.

We have gone to great lengths to make sure that personal data is not disclosed through the notification process of a hack. I understand that the personal data has already been accessed by the individual who committed the act, but we want to make sure that the government doesn't contribute to the distribution of that data.

In order to create an incentive in a voluntary program for a business to initiate that notification to the Federal Government, we provide liability protection. Anytime a company allows personal data or data on their business to get out, there could potentially be a shareholder's suit. What we do is provide a blanket liability protection to make sure that a company can't be sued for the government notification of a security breach where data has been removed and it is in the best interest of the government to know it, to react to it, and for the general population of businesses in America to understand it.

So we have business-to-business collaboration with your competitor, anti-trust protection, business-to-government liability protection, no personal data transmitted, and the last piece is government to business.

It is hard for me to believe that the government didn't have the statutory authority to convey to businesses across America when a cyber attack is in progress. The Federal Government has to be asked to come in and typically will be asked by the company that has been attacked, but how about their competitors? How about the industry sector? How about the whole U.S. economy? There is no authority to do that. This bill creates the authority in the Federal Government to receive that information from a company that has been penetrated, to process it, to understand who did it, to understand the attack tool they used, to determine the defensive mechanism of software that it can be put on, and then to notify American businesses that there is an attack happening now, and here is the attack tool and software you can buy off the shelf and put on your computer system to protect you. That is it. That is the entire information sharing bill, and it is voluntary.

I will touch on eight items very briefly. Why is there a need for cyber legislation? I don't want to state the obvious, but we have already seen that individuals and nation states penetrate the private sector and steal personal data, and the Federal Government can steal personal data. I thought it would hit home with my colleagues when the Office of Personnel Management was breached, and now we are up to 22 to 24 million individuals who were compromised. More importantly, the personal data at OPM extended to every individual who had ever applied for a security clearance, who had ever been granted security clearance, and who had security clearances and are now retired, but for some reason that application remained in the database. That application, which consists of 18 pages, has the most personal information one can find. It lists your parents and their Social Security numbers, your brothers, your sisters, where you lived since you graduated from college. It even has a page that asks you to share the most obvious way that someone might blackmail you. It has probably some of the most damaging personal information that one can have breached.

Cyber attacks have harmed multiple U.S. companies. If this weren't serious, would the President of China and the President of the United States, when they met several weeks ago, have come to an agreement about how they would intercede if one country or the other commits a cyber attack against each other? Probably not.

Our bill is completely voluntary, and I think it is safe to say that those who want to share data can, in fact, share data on this.

I mentioned the words ''real time.'' What we want to do is create a real-time system because we want a partnership. We want a partnership with other private companies and we want a partnership with the private and public sector, and you can't get a partnership by mandating it. All you can get is an adversarial relationship. We maintain that voluntary status in the hope that the sharing of that information is, in fact, real time. We can control—once you transmit to the Federal Government—how to define ''real time.'' I have no control over a private company's decision once they know they have been breached to the point that they actually make a notification to the Federal Government, but with the liability protection and anti-trust coverage, we are convinced that we are structured from the beginning to create an incentive for real time to take place.

We protect personal privacy. Many have come to the floor and have suggested that this is a surveillance bill. Let me say to my colleagues and to the American people: There is no capability for this to become a surveillance bill. The managers' amendment took those items that people were concerned with and eliminated it. We can be accused of a lot of things, but to accuse this of being a surveillance bill is either a sign of ignorance or a sign that one is being disingenuous. It is not a surveillance bill. Be critical of what we are attempting to do, be critical of what we do, but don't use the latitude to suggest that this is something that it is not.

We require private companies and the government to eliminate any irrelevant personal, identifiable information before sharing the cyber threat indicators or putting up defensive mechanisms.

This bill does not allow the government to monitor private networks or computers. It does not let government shut down Web sites or require companies to turn over personal information.

This bill does not permit the government to retain or use cyber threat information for anything other than cyber security purposes, identifying a cyber security threat, protecting individuals from death or serious bodily or economic harm, protecting minors, or investigating limited cyber crime offenses.

This bill provides rigorous oversight and requires a periodic interagency inspector general's report to assess

whether the government has violated any of the requirements in this bill. The report also will assess any impact this bill may have on privacy and civil liberties. In the report, we require the IG to report to us whether anybody does anything outside what the statute allows them to do, but we also ask the IG to make a gut call on whether we have protected privacy and civil liberties.

Finally, our managers' amendment has incorporated an additional provision to enhance privacy protections first. Our managers' amendment omitted the government's ability to use cyber information to investigate and prosecute serious and violent felonies. Let me raise my hand and say I am guilty. I felt very strongly that that should have been in the bill. If we find during an investigation that an individual has committed a felony that is not related to a cyber attack, I thought we should turn that information over to law enforcement but, no, we dropped it. I don't want there to be any question as to whether this is an effective cyber information sharing bill.

Our managers' amendment limited cyber threat information sharing authorities to those items that are shared for cyber security purposes. Both of these changes ensure that nothing in our bill reaches beyond the focus of cyber security threats that are intended to prevent and deter an attack, and nothing in this bill creates any potential for surveillance authorities.

Now, as I said, despite rumors to the contrary, this bill is voluntary. It is a voluntary threat indicator to share with authorities and does not provide in any way for the government to spy on or use library and book records, gun sales, tax records, educational records, or medical records. There is something in that for every member of every State.

I can honestly look at my librarians and say we haven't breached the public libraries' protection of personal data. I will say librarians are not fans of this legislation. I don't think they have read the managers' amendment that spells out the concerns we heard and then said: This can't go there. I am not sure we can statutorily state it any clearer than what we have done.

Given that cyber attackers have hacked into, stolen, and publicly disclosed so much private, personal information, it is astounding to me that privacy groups would oppose this bill. It has nothing to do with surveillance, and it seeks to protect private information from being stolen.

There are no offensive measures. This bill ensures that the government cannot install, employ or otherwise use cyber security systems on private sector networks. In other words, no one can hack back into another computer, even if the purpose is to protect against or squash a cyber attack. It can't be done. It is illegal.

The government cannot retain or use cyber threat information for anything other than cyber security purposes, including preventing, investigating, disrupting, and prosecuting limited cyber crimes, protecting minors, and protecting individuals from death or serious bodily harm, or economic harm.

The government cannot use cyber threat information in regulatory proceedings. Let me state that again. The government cannot use cyber threat information in regulatory proceedings. If somebody believes this is not voluntary and that there is some attempt to try to get a mandatory hook in here where regulators can turn around and bypass the legislative responsibility of the Congress of the United States, let me just say, we are explicit. It cannot be done. But we are also explicit that the government cannot retain this information for anything other than the list of items I discussed. This provides focused liability protection to private companies that monitor their own systems and share cyber threat indicators and defensive mechanisms in accordance with the act, but the liability protection is not open-ended. This doesn't provide liability protection for a company that engages in gross negligence or willful misconduct. I am not a lawyer, but I have been told that ties it up pretty tightly; that it makes a very small, narrow lane that companies can achieve liability protection, and that lane means they are transferring that information to the Federal Government.

Last, independent oversight. This bill provides rigorous oversight. It requires a periodic interagency inspector general's report to assess whether the government has violated any of the requirements of this act. The report also will assess any impact that this bill may have on privacy and civil liberties as well as an assessment of what the government has done to reduce any impact.

This bill further requires an independent privacy and civil liberties oversight board to assess any impact this bill may have on privacy and civil liberties and is, in fact, reviewed internally by an inspector general. The inspector general checks to make sure they live by the letter of the law. The inspector general makes an assessment on the privacy and civil liberties, and we set up an independent board to look at whether, in fact, privacy and civil liberties have been protected.

I say to my colleagues, if there is more that they need in here, tell us what it is. The amendment process is open.

Here is where we are. Privacy folks don't want a bill, period. Some Members don't want a bill, period. I get it. I am willing to adapt to that. I only need 60 votes for this to pass, and then I have to conference it with the House that has two different versions. Then I have to go to the other end of Pennsylvania Avenue, and I have to convince the President and his whole administration to support this bill. Let me quote the Secretary of the Department of Homeland Security. They support this bill. The National Security Council tomorrow is going to come out in support of this bill. Why? Because most people recognize the fact that we need this, that this is the responsible thing to do. This is why Congress was created.

If, in fact, there are those who object, don't participate. I say to those businesses around the country, I am not going to get into your decisionmaking, although I think it is flawed. You hold most of the personal data of any companies out there. Yet you don't want to see any coordinated effort to minimize data loss in the U.S. economy. I think that is extremely shortsighted. I think your customers would disagree with you, but the legislation was written in a way that allows you to opt out and to say: I don't want to play in this sandbox.

I say to my colleagues and to the American people: Is that a reason for us not to allow the thousands of companies that want to do it, representing hundreds of thousands and millions of customers who want to protect their credit card number, their health records, all the personal data that is out there on them—if they want to see that protected, should they not have that done because some companies say they don't want to play? No. We make it voluntary, and we allow them to opt out. They can explain to their customers why. If I am with another tech company and they are participating in this, they must be more interested in protecting my data. I think it is a tough sell myself as a guy in business for 17 years.

I know what is up here. Some are looking at this as a marketing tool. They are going to go out and say: We don't participate in transferring data to the Federal Government. Oh, really. Wait until the day you get penetrated. Wait until the day they download all of that personal information on all of your customers. You are going to be begging for a partnership with the Federal Government. Then we are going to extend it to you, whether you liked it or not, whether you voted for the bill or supported the bill or spoke in favor of the bill or ever participated in it. If we pass this bill, which I think we will, they will have an opportunity to partner with the Federal Government and to do it in an effective way. In the meantime, I think there will be just as many businesses using a marketing tool that says: We like the cyber information sharing bill, and if we ever need to use it, we are looking forward to partnering with the Department of Homeland Security, the FBI, and the National Security Agency because we want to minimize the exposure of the loss of data our customers could have.

Mark my words. There is a real battle getting ready to brew here. Again, putting on my business hat, I like the idea of being able to go out and sell the fact that I am going to partner if something happens much better than selling

the pitch that I am going to do this alone. Think about it. A high school student last week hacked the personal email account of the Secretary of the Department of Homeland Security and the Director of the CIA. This is almost ''Star Trek.'' ''Beam me up, Scotty.''

There are people who believe that this is just going to go away. It is not going away. Every day there is an attempt to try to penetrate a U.S. company, an agency of the Federal Government for one reason: to access personal data. The intent is there from individuals and from nation states. For companies that think this is going to go away or think they are smart enough that it is not going to happen to them, I have seen some of the best and they are one click away from somebody downloading and entering their system and that click may not be protected by technology. It may be the lack of ability of an employee to make the right decision on whether they open an email, and, boom, they have just exposed everybody in their system.

So I will wrap up because I see my good friend and colleague Senator WYDEN is here. We will have several days, based upon the process we have in front of us, to talk about the good, and some will talk about the bad, which I don't think exists, but let me assure my colleagues that the ugly part of this—the ugly part of this—is that cyber theft is real. It doesn't discriminate. It goes to where the richest pool of data is. In the case of the few companies that are not supportive of this bill, they are the richest depositories of personal data in the world. I hope they wake up and smell the roses.

I yield the floor.

The PRESIDING OFFICER (Mr. SCOTT). The Senator from Oregon.

Mr. WYDEN. Mr. President, I would like to inform my colleague, the distinguished chairman of our Intelligence Committee, I am always thinking about the history of the committee. I believe Chairman BURR, the ranking minority member Senator FEINSTEIN, and I have been on the Intelligence Committee almost as long as anybody in history.

I always like to work with my colleague. This is an area where we have a difference of opinion. I am going to try to outline what that is and still try to describe how we might be able to work it out.

Mr. BURR. May I thank my colleague?

Mr. WYDEN. Of course.

Mr. BURR. Mr. President, I thank my colleague. I think he diplomatically referred to me as old, but I know that wasn't the case. He is exactly right. We have served together for a long time. We agree on most issues. This is one that we disagree on, but we do it in a genuine and diplomatic way. Contrary to maybe the image that some portray to the American people, we fight during the day and we can have a drink or go to dinner at night, and we are just as likely to work on a piece of legislation together next week. So that is what this institution is and it is why it is so great.

Mr. WYDEN. Well said. There is nothing better than having Carolina barbecue unless it is Oregon salmon. Yes, we old jocks, former football players and basketball players, we have tough debates and then we go out and enjoy a meal.

Here is how I would like to start this afternoon. The distinguished chairman of the committee is absolutely correct in saying that cyber security is a very substantial problem. My constituents know a lot about that because one of our prominent employers, SolarWorld, a major manufacturer in renewable energy, was hacked by the Chinese simply because this employer was trying to protect its rights under trade law. In fact, our government indicted the People's Liberation Army for their hacking into this major Oregon employer. So no question that cyber security is a major problem.

Second, there is no question in my mind that information sharing can be very valuable in a number of instances. If we know, for example, someone is associated with hackers, malware, this sort of thing, of course it is important to promote that kind of sharing. The difference of opinion is that I believe this bill is badly flawed because it doesn't pass the test of showing that when we share information, we have to have robust privacy standards or else millions of Americans are going to look up and they are going to say that is really not cyber security. They are going to say it is a surveillance bill. So that is what the difference of opinion is.

AMENDMENT NO. 2621, AS MODIFIED

Let me turn to how I have been trying to improve the legislation. I am going to speak for a few minutes on my amendment No. 2621 to the bill that we have been discussing and that is now pending in the Senate. Obviously, anybody who has been watching the debate on this cyber security bill has seen what we would have to call a spirited exchange of views. Senators are debating the substance of the legislation and, as I just indicated to Chairman BURR and I have indicated to ranking minority member Senator FEINSTEIN, there is agreement on a wide variety of points and issues.

Both supporters and opponents of the bill agree that sharing information about cyber security threats, samples of malware, information about malicious hackers, and all of this makes sense and one ought to try to promote more of it. Both supporters and opponents now agree that giving corporations immunity from customer lawsuits isn't going to stop sophisticated attacks such as the OPM personnel records breach.

I am very glad that there has been agreement on that point recently, because proponents of the bill sometimes said that their legislation would stop hacks such as the one that took place at OPM. When technologists reviewed it, that was clearly not the case, and the claim has been withdrawn that somehow this bill would prevent hacks like we saw at OPM.

The differences of opinion between supporters and opponents of the bill—who do agree on a variety of these issues—surround the likely privacy impact of the bill. Supporters have essentially argued that the benefits of this bill, perhaps, are limited—particularly now that they have withdrawn the claim that this would help against an OPM attack—but that every little bit helps. But there is no downside to them to just pass the bill. It makes sense. Pass the bill. There is no downside.

Opponents of the bill, who grow in number virtually every day, have been arguing that the bill is likely to have a significant negative impact on the personal privacy of a large number of Americans and that this greatly outweighs the limited security benefits. If an information sharing bill doesn't include adequate privacy protections, I am telling you, colleagues, I think those proponents are going to have people wake up and say: I really don't see this as a cyber security bill, but it really looks to me like a surveillance bill by another name.

(Mr. TOOMEY assumed the Chair.)

Colleagues who are following this and looking at the bill may be trying to sort through this discussion between proponents and opponents. To help clarify the debate, I would like to get into the text of the bill for just a minute.

If colleagues look at page 17 of the Burr-Feinstein substitute amendment, which is the latest version with respect to this bill, Senators are going to see a key section of the bill. This is the section that discusses the removal of personal information when data is shared with the government. The section says very clearly that in order to get immunity from a lawsuit a private company has to review the data they would provide and remove any information the company knows is personal information unrelated to a cyber security threat. This language, in my view, clearly creates an incentive for companies to dump large quantities of data over to the government with only a cursory review. As long as that company isn't certain that they are providing unrelated personal information, that company gets immunity from lawsuits. Some companies may choose to be more careful than that, but this legislation and the latest version—the Burr-Feinstein substitute amendment—would not require it. This bill says with respect to personal data: When in doubt, you can hand it over.

My amendment No. 2621 is an alternative. It is very simple. It is less than a page long. It would amend this section that I have just described to say that when companies review the data they provide, they ought to ''remove, to the extent feasible, any personal information of or identifying a specific

individual that is not necessary to describe or identify a cybersecurity threat.'' The alternative that I am offering gives companies a real responsibility to filter out unrelated personal information before that company hands over large volumes of personal data about customers or people to the government.

The sponsors of the bill have said that they believe that companies should only give the government information that is necessary for cyber security and should remove unrelated personal information. I agree with them, but for reasons that I have just described, I would say respectfully that the current version of this legislation does not accomplish that goal, and that is why I believe the amendment I have offered is so important.

For an example of how this might work in practice, imagine that a health insurance company finds out that millions of its customers' records have been stolen. If that company has any evidence about who the hackers were or how they stole this information, of course it makes sense to share that information with the government. But that company shouldn't simply say here you go, and hand millions of its customers' medical records over for distribution to a broad array of government agencies.

The records of the victims of a hack should not be treated the same way that information about the hacker is treated. Companies should be required to make a reasonable effort to remove personal information that is not needed for cyber security before they hand information over to the government. That is what my amendment seeks to achieve. That is not what is in the substitute amendment.

Furthermore, if colleagues hear the sponsors of the substitute saying this bill's privacy protections are strong and you have heard me making the case that they really don't have any meaningful teeth and they are too weak, don't just take my word for it. Listen to all of the leading technology companies that have come out against the current version of this legislation.

These companies know about the importance of protecting both cyber security and individual privacy. The reason they know—and this is the case in Pennsylvania, Oregon, and everywhere else—is that these companies have to manage the challenge every single day. Companies in Pennsylvania and Oregon have to ensure they are protecting both cyber security and individual privacy. Those companies know that customer confidence is their lifeblood and that the only way to ensure customer confidence is to convince customers that if their product is going to be used, their information will be protected, both from malicious hackers and from unnecessary collections by their government.

I would note that there is another reason why it is important to get the privacy protections I am offering in my amendment at this time. The companies that I just described are competing on a global playing field. These companies have to deal with the impression that U.S. laws do not adequately protect their customers' information. Right now these companies—companies that are located in Pennsylvania and Oregon—are dealing with the fallout of a decision by a European court to strike down the safe harbor data agreement between the United States and the European Union. The court's ruling was based on the argument that U.S. laws in their present form do not adequately protect customer data. Now, I strongly disagree with this ruling. At the same time, I would say to my colleagues and to the Presiding Officer—he and I have worked closely on international trade as members of the Finance Committee—and I would say to colleagues who are following this international trade question and the question of the European Union striking down the safe harbor for our privacy laws, in my view this bill is likely to make things even more difficult for American companies that are trying to get access to those customers in Europe.

To give just a sampling of the leading companies that have come out against the CISA legislation, let me briefly call the roll. There is the Apple company. They have millions of customers. They know a great deal about what we have to do to deal with malicious hackers and to protect privacy. There is also Dropbox, Twitter, Salesforce, Yelp, Reddit, and the Wikimedia Foundation. I point to the strong statement by the Computer & Communications Industry Association. Their members include Google, Amazon, Facebook, Microsoft, Yahoo, Netflix, eBay, and PayPal. Those individual companies I have mentioned have millions of customers. The organization that speaks for them says: ''CISA's prescribed mechanism for sharing of Cyber threat information does not sufficiently protect users' privacy.''

On top of this, there has been widespread opposition from a larger spectrum of privacy advocacy organizations. Here the groups range from the Open Technology Institute to the American Library Association.

I was particularly struck by the American Library Association's comments in opposition to this bill. I think the leadership said—paraphrasing—something to the effect of when the American Library Association opposes legislation that authors say will promote information sharing, they indicate there was a little something more to it than what the sponsors are claiming.

Wrapping up, I want to make clear, as I said yesterday, that I appreciate that the bipartisan leadership of our committee has tried to respond to these concerns. They know that these large companies with expertise in collecting data and promoting cyber security have all come out against the bill. I heard talk about privacy protections. I don't know of a single organization that is looked to by either side of the aisle, Democrats and Republicans, for expertise and privacy that has come out in favor of the bill.

So the sponsors of this legislation and the authors of the substitute amendment, which I have tried to describe at length here this afternoon, are correct in saying that they have made some changes, but those changes do not go to the core of the bill.

For example, the amendment I have described would really, in my view, fix this bill by ensuring that there was a significant effort to filter out unrelated personal and private information that was sent to the government under the bill.

So I hope Senators will listen to what groups and the companies that have expertise in this field have said. I hope Senators on both sides of the aisle will support the amendments I and others have offered. The Senate needs to do better than to produce a bill with minimal effects on the security of Americans and significant downside for their privacy and their liberty.

I yield the floor.

The PRESIDING OFFICER. The Senator from Rhode Island.

AMENDMENT NO. 2626, AS MODIFIED

Mr. WHITEHOUSE. Mr. President, I would like to speak for 5 or 6 minutes on the cyber bill.

Unfortunately, I am here to express my distaste for the manner in which this bill has proceeded. I have an amendment that is not going to be voted on. Let me describe some of the characteristics of that amendment.

First of all, it is bipartisan. It is Senator GRAHAM's and my amendment.

Second, it has had a hearing. We have had a hearing on it in the Judiciary Committee. Considerable work has gone into it.

Third, it has the support of the Department of Justice. It repairs holes in our criminal law for protecting cyber security that we worked on very carefully with the Department of Justice and which we have had testimony in support of from our Department of Justice prosecutors.

Last, it was in the queue. It was in the list of amendments that were agreed to when we agreed to go to the floor with this bill.

So I don't know how I am going to vote on this bill now. But if you have a bipartisan amendment that has had a hearing, that was in the queue, and that has the support of the Department of Justice and you cannot even get a vote on it, then something has gone wrong in the process.

I remember Senator SESSIONS coming to the floor and wondering how it is that certain Senators appoint themselves masters of the universe and go off in a quiet room someplace and decide that certain amendments will and will not be heard. I am very sympathetic to Senator SESSIONS' concerns right now.

Let me tell you what the substance of our amendment would do.

First, there are people out there around the world in this cyber universe of fraud and crime who are trafficking in Americans' financial information for purposes of fraud and theft. If they don't travel to America or if they don't have a technical connection to America, we cannot go after them. There is an American victim, but we cannot go after them. That is a loophole that harms Americans that this bill would close.

I cannot believe there is one Member of this institution who would oppose closing a loophole that allows foreign criminals access to Americans' financial information for fraudulent purposes but puts them beyond the reach of our criminal law. That is one part of what our bill does.

Second, it raises penalties for people who intrude on critical infrastructure. You can go all around this country, you can go to military installations that have way less security concerns than our critical infrastructure, like our electric grid, and you will see chain-link fences that say department of whatever, U.S. Government, stay out. You cannot go in there to picnic, you cannot go in there because you are curious, you cannot go in there for a hike, and the reason is because there is a national security component to what is going on in there.

Well, there is a huge national security component to our critical infrastructure, like our electric grid. All this would do is raise the penalties. You could still go in, but if you get caught doing something illegal there, then it is a little different if you are attacking America's critical infrastructure than if you are just prowling around in some other portion of the Web that does not have that.

Again, I think if that came to a vote, we would probably get 90 percent of this body in favor. Who is in support of allowing people to mess around in our critical infrastructure?

The third is botnet brokers. Botnets are out there all over the Internet. They are a plague on the Internet. There is no such thing as a good botnet. Everyone would be better off if they were removed. They are like weeds on the Internet. There are people who are brokers who allow access to botnets, and because our laws are so out of date, if you are just brokering access to a botnet for criminal purposes, there is no offense. Why would we not want to empower our Department of Justice to be able to go after people who are criminal brokers allowing access for criminals to botnets to use for criminal purposes against Americans? I don't understand that.

Lastly, botnet takedowns. A botnet is a weed. We wait until somebody actually encounters that weed and is harmed by it before we allow our Department of Justice to act. We should be out there taking down botnets on a hygiene basis all the time. We are limited because of this artificiality. That is the fourth piece of the bill. It empowers botnet takedowns like the Bugat takedown we just did. We should be doing a lot more of that. Again, unless somebody here is in the botnet caucus and is in favor of more botnets out there, this is something which would probably pass unanimously. Yet I cannot get a vote.

It is bipartisan, has had a hearing, is in the queue, is supported by the Department of Justice, and those are the four sub-elements of it. For some reason, the masters of the universe have gone off and had a meeting in which they decided this is not going to be in the queue. I object to that procedure.

I am sorry we are at this stage at this point because I think that on the merits this would win. This is a bipartisan, good, Department of Justice-supported, law enforcement exercise to protect people against cyber criminals. I don't know what the sense is that there is some hidden pro-botnet, pro-foreign cyber criminal caucus here that won't let an amendment like mine get a vote.

I will yield the floor. I see Senator CARPER here, and he has done great work to try to be more productive than my amendment reflects. I hope we can sort this out to a point where an amendment like mine, which was in the queue in the original deal that got us to this bill, can now get back in some kind of a queue so that we can get this done.

I yield the floor.

The PRESIDING OFFICER. The Senator from Delaware.

Mr. CARPER. I appreciate the yielding by Senator WHITEHOUSE. Let me just say that if your provision, Senator WHITEHOUSE, does not end up in this bill and we actually do pass it, I am sure we will conference with the House. There will be an opportunity to revisit this issue. So I hope you will stay in touch with those of us who might be fortunate enough to be a conferee.

Mr. WHITEHOUSE. I appreciate that very much, more than the Senator can know.

Mr. CARPER. Mr. President, I rise today in support of the cyber security information bill introduced by my colleagues, Senators BURR and FEINSTEIN. I want to commend my colleagues and their staff for their leadership and for their tireless efforts on this extremely important piece of legislation.

As ranking member and former chairman of the Homeland Security and Governmental Affairs Committee, I have been following cyber security and this information sharing proposal in particular literally for years. In fact, when Senator FEINSTEIN first introduced an information sharing bill in 2012—that was like two or three Congress's ago—it was referred to Homeland Security and Governmental Affairs, on which I served. That bill was ultimately folded into a comprehensive cyber security bill that I had the honor of cosponsoring with Senators Joe Lieberman, SUSAN COLLINS, Jay Rockefeller, and Senator FEINSTEIN. We were not able to pass that bill, but I think it has paved the way for other cyber legislation, including the bill that is before us today and a number of the amendments that are going to be offered to that bill in the managers' amendment, especially.

Last Congress, I worked with our ranking member on homeland security, Dr. Tom Coburn, and our House counterparts to get not one, not two, not three, but four cyber security bills enacted into law, signed by the President. I believe these four bills laid a very strong foundation for some significant improvements on how the Department of Homeland Security carries out its cyber security mission and really for this bill before us too.

What the legislation Dr. Coburn and I worked on during the last Congress did, in essence, was to better equip the Department of Homeland Security to operate at the center of the kind of robust information sharing program that the Burr-Feinstein bill would set up. How do they do that? One, make sure the Department of Homeland Security would have the ability to attract and retain top-flight talent, much like the National Security Agency already has.

The legislation actually takes something called the cyber ops center, NCCIC, within the Department of Homeland Security and makes it real and functional and an entity that people would use and listen to.

Finally, we took an old law called FISMA, the Federal Information Sharing Management Act—we took something that was just a paperwork operation, this FISMA legislation—like a once-in-a-year check to see how good a cyber security agency might be—and turned it into not a paperwork operation, not a once-every-365-days operation, but a 24/7 surveillance operation on the lookout for intrusions within and across the Federal Government broadly.

That legislation, affectionally known as FISMA, was also designed to make clear what the division of labor was between the Office of Management and Budget, OMB, and the Department of Homeland Security on protecting the dot.gov domain. We made it clear that the job of OMB is to, if you will, steer the ship. The job of the Department of Homeland Security is to row the ship, to row the boat. That is a good division of labor given that OMB only has six employees who work on this stuff and the Department of Homeland Security has hundreds. So I think we figured out the sharing of labor, the division of labor, and also made sure the Department of Homeland Security has the resources—the horses, the resources—and the technology they need.

Sharing more cyber security threat information among and between the private sector and the Federal Government players who are on the frontline in cyber security is critical for national security. Over the last couple of

years, we have witnessed many troubling cyber attacks against our banks, but not just our banks, against retailers, health providers, government agencies, and God knows how many others.

Some of those launching these attacks were just criminals. Some of them were just criminals. They want to steal information. They want to make money off of our personal information, off our intellectual property, like our intellectual seed corn, if you will, for companies large and small and for universities as well. Others just want to be disruptive or they want to make political points. Some actors, however, are capable or would like to develop the capability to use a cyber attack to harm people and cause physical damage.

It is long past time for this body to take action to more effectively combat these threats we now face in cyber space. That is why earlier this year I introduced a similar information sharing bill. This bill largely mirrored the administration's original proposal.

The administration asked me to introduce their information sharing bill. Before I did that, we actually had a hearing in the committee on homeland security. Part of the centerpiece of the hearing was the administration's proposal. We got some good ideas on how to make it better. We made it better and introduced that bill to use, if you will, as a point-counter point in a constructive, positive way with the legislation that worked its way through the Intelligence Committee. But we did not stop there. We took information from a lot of experts and stakeholders.

The measure we are discussing today shares the same goals as my original bill—largely the administration's original bill—to increase the sharing of cyber threat information between the Federal Government and the private sector and between different entities within the private sector. I am pleased that we are finally discussing these critical issues on the Senate floor.

The substitute amendment we are debating today makes a number of improvements to the bill that was first made public after the Intelligence Committee reported it out. It also includes several changes that I, as well as several of my colleagues, have been calling for—including the chairman of our committee.

I would like to thank Senators BURR and FEINSTEIN. I thank their staff for working closely with our staff and others to produce what I believe is a significantly smarter and stronger bill. Is it perfect? No, not yet. But I can say there is always room for improvement. That is why we still have a debate on a number of amendments and those like the one mentioned by Senator WHITEHOUSE that may be germane in a different kind of way in conference.

While there may not be agreement on everything in this bill, I believe most of our colleagues would come to the conclusion that it really will help to improve our Nation's cyber security and, by extension, our national security and, by extension, our economic security.

First, the bill would ensure that the government—our government—is providing actionable intelligence to private sector entities that are seeking to better protect themselves in cyber space. Businesses around our country are hungry for information they can use to fend off attacks and better protect their systems and their customers. This bill would make the Federal Government a much stronger partner for them.

Many companies that I have talked to of late also want to share more information with the Federal Government about what they are seeing online every day, but they are unsure of the rules of the road. In other words, companies want more predictability and they want more certainty when it comes to working with our government. This bill would give them that by clarifying that they won't be putting themselves in legal jeopardy if they choose to share cyber threat information with our Federal Government.

If companies do want to avail themselves of the legal protections the bill offers, they would have to, with two narrow exceptions, use the information sharing portal at the Department of Homeland Security. This puts the Department of Homeland Security, a civilian entity, at the center of the information sharing process. I think this is smart and the right thing to do. In fact, many experts and companies that I have talked to across the country as recently as last week out in Silicone Valley and out on the west coast—they agree with what I have just said.

I know many Americans are uneasy with companies they do business with directly handing over data to an intelligence or law enforcement agency. The Department of Homeland Security will carry out its responsibilities under this bill through the cyber ops center I mentioned earlier called the National Cyber Security and Communications Integration Center—that is a mouthful. We affectionately call it N-Kick. It is the cyber ops center. It includes folks from DHS and other Federal agencies. It includes a number of representatives of financial services, the utility industry, our retail industry, and so forth, all together under one roof, talking together and working together to help us support one another and make it strong and more secure.

One of the bills I worked on with Dr. Coburn last Congress formally, as I said earlier, authorized this center. We are pleased to see that this bill would make the most out of the resources we have already invested in this cyber ops center, NCCIC.

Earlier this month, Secretary Jeh Johnson of the Department of Homeland Security told our Homeland Security and Governmental Affairs Committee that beginning in November, the cyber ops center, NCCIC, will have the capability to automate the distribution and receipt of cyber threat indicators. I will say that again—to automate the distribution and the receipt of cyber threat indicators that they receive from others, including those in the private sector. In other words, the Department of Homeland Security will have the ability to share information with other agencies in real time—not next month, not next week, not tomorrow, not in an hour, but in real time, which is really what this little bill before us today requires.

I know that the real-time sharing is incredibly important to the bill's sponsors, and it is important to me and probably to many of our colleagues and stakeholders. Equally important, however, is the ability of the Department of Homeland Security to apply what I call a privacy scrub to the information it receives from industry, the threat indicators that come from industry—see something, say something—stuff that they send to the Department of Homeland Security.

In the bill that I authored with others in my committee, including our chairman, we allow the Department of Homeland Security to, if you will, receive information through its portal from various entities that witness threat indicators, to see it and to put it through the portal, to bring it through the portal to do a privacy scrub. That is one of the things the Department of Homeland Security has expertise in doing.

I used an example at lunch earlier today. I talked about baseball. I know the Presiding Officer has some interest in baseball. There are teams called the Phillies in Philadelphia and the Pirates in Pittsburgh. I would just say to him, thinking about baseball for a minute, let's say you are in the playoffs. Let's say you have a team in the playoffs. You are in the ninth inning, and you need to get somebody out of the bullpen to close. You have a one-run lead. You look to the bullpen. He is now retired, but Mariano Rivera was the best closer in baseball history. You have Mariano Rivera in the bullpen to come in and close the game, and you have three other guys you just called up from the Minor League, so maybe from AAA.

You say: Well, whom do I put in to close the game? Do I put in the best closer we have ever had in baseball history or do I bring in three rookies, three Minor League guys?

Well, you bring in Mariano Rivera.

When it comes to being able to do privacy scrubs, the Department of Homeland Security—that is what they do. That is what they do. Now they have the horses, the ability, and the technology to do it even better.

I know some of my colleagues are concerned that a privacy scrub will slow down the information sharing process. I share those concerns, but I have been assured by the Department—the bright, smart people at the Department of Homeland Security—that less

than 1 percent of the information it receives would actually ever need to be reviewed by a human, by a person. The rest—roughly 95 percent to 99 percent—would be shared with other agencies at machine speed. Bingo.

I am very pleased that DHS has come to an agreement on this process with its agency partners. We will be up and running with a portal in the way I have described in the next couple weeks.

One of the amendments I filed speaks to this privacy scrub process. It would make clear that the Department of Homeland Security could carry out an automated privacy scrub in real time and without delay. In fact, my amendment would add just one word to the bill so that DHS could continue to automatically remove irrelevant or erroneous data from cyber threat information.

I am very pleased that Senators BURR and FEINSTEIN have taken this amendment into consideration and have now modified their substitute amendment to make sure the Department of Homeland Security can do what it does best, and that is to apply a privacy scrub—pulling out personally identifiable information that actually shouldn't be passed on to other Federal agencies. The substitute amendment now calls on DHS to work with its agency partners to agree on a process to share information while protecting privacy. This is a process DHS is already undertaking.

I thank Senators BURR and FEINSTEIN, as well as our friends at the Department of Homeland Security and other agencies, for working so hard to find agreement on this language and for working with my staff and me on this important matter.

Another amendment I put forward with our committee chairman, Senator JOHNSON, aims to improve what we call cyber hygiene across the Federal Government and to prevent attacks against Federal agencies. This language is based on a bill that Senator JOHNSON and I introduced and had reported out of our homeland security committee by a unanimous vote. The amendment does three main things.

First, it would require all Federal agencies to implement specific best practices and state-of-the-art technologies to defend against cyber attacks. For example, we had experts testify about the importance of strong authentication and data encryption. This amendment would make sure that agencies are taking these commonsense steps to bolster their cyber security defenses.

Second, the amendment would accelerate the deployment and adoption of the Department of Homeland Security's cyber intrusion and detection program, known as EINSTEIN, as in Albert Einstein, but you don't have the ''Albert'' in the name of this technology; it is called EINSTEIN.

For my colleagues who may not be familiar with EINSTEIN, with respect to homeland security and cyber security, let me take a couple of minutes to describe its main features.

We had EINSTEIN 1 present at the beginning, EINSTEIN 2 was follow-on technology, and then there is EINSTEIN 3. EINSTEIN basically analyzes Internet traffic entering and leaving Federal civilian agencies to identify cyber threats and to try to stop attacks.

This system has been rolled out in phases over the last several years. EINSTEIN 1 is the first step. It sees and actually records Internet traffic, much like a guard at a checkpoint watches cars go by and maybe writes down and records the license plates. EINSTEIN 2 detects anything out of the ordinary and sets off alarms if a piece of malware is trying to enter a Federal network. For example, a car comes through and it is not supposed to come through. That would set off an alarm and enable EINSTEIN 2 to actually detect a cyber intrusion. It doesn't do anything about blocking. It doesn't block the car, in this example. It doesn't block anything. EINSTEIN 3A, the latest version, uses unclassified and classified information to actually block the cyber attack.

So initially EINSTEIN 1 records basically what is being detected, EINSTEIN 2 actually detects bad stuff coming through in terms of an intrusion, and EINSTEIN 3A blocks it. The problem is that less than half of our Federal civilian agencies actually have EINSTEIN 3A in place. They have the ability to record an intrusion, the ability to detect an intrusion, but not the ability to block an intrusion. They need the ability to block. What our legislation would do would be to make sure that agencies have EINSTEIN in place, including the ability to block intrusions, within 1 year.

Finally, our amendment incorporates the language originally drafted by Senator SUSAN COLLINS, the former chair of the homeland security committee and a great colleague of ours for many years, Senator MARK WARNER, Senator KELLY AYOTTE, Senator CLAIRE MCCASKILL, Senator DAN COATS, and Senator BARBARA MIKULSKI. They are all cosponsors of the amendment Senator COLLINS offered. These provisions would strengthen the ability of the Department of Homeland Security to shore up cyber defenses at civilian agencies and to address cyber emergencies across the Federal Government.

Again, I am incredibly grateful that Senator FEINSTEIN and Senator BURR agreed to include our language in the substitute amendment language that worked its way through our committee. We had hearings and had the opportunity to mark up the legislation. It worked the way it is supposed to work. And I think that without exception it had bipartisan support coming through our committee. It is the perfect complement to the information sharing bill we are discussing this week. I think it makes a good bill that much better.

I thank the Senators for working with me and Senator JOHNSON on it.

Just one more thing before I close. I know the Presiding Officer thinks a lot about root causes, and rather than just address the symptoms of a problem, let's think about what is the root cause of the problem. The Senator who is waiting to follow me on the floor, the former Governor of Maine, thinks similarly. I do too. It is not enough to just address the symptoms of these problems. A part of what we need to be thinking about is, How do we get to the root cause?

Until fairly recently, a lot of our financial services institutions in this country were under constant attack by somebody who was trying to overload their Web sites and essentially trying to shut them down. It is sort of like when we were first standing up the Affordable Care Act, they had so much traffic on their Web site that it would kind of break down.

There are so many cyber threats from around the world. We think Iran is behind it. They are trying to do that, to bring down our financial services business—and sometimes with some success.

About a year ago, when we got very serious about negotiating with the Iranians and our partners—the French, the Brits, the Germans, the Russians, and the Chinese—some kind of an agreement where the Iranians would give up any hope they had of having a nuclear weapon and the terms for our lifting our economic sanctions—when it became clear that those were serious negotiations, that something might actually happen from those negotiations, guess what happened to those attacks. We call them DDoS. What do you suppose happened? Well, guess what, they started letting up little by little until the time we actually voted here to let that agreement be enacted and hopefully be administered and implemented. That was a root cause being addressed.

Another root cause we had over in China—for years the Chinese have sought to use cyber attacks to get into our most successful businesses, some of our research and development operations in those businesses, and work being done within Federal agencies on research and development—actually, the intellectual seed corn for creating jobs and opportunity in this country. The cyber attacks were—we believe it was China trying to steal information from our universities. They were doing a lot of research that could lead to economic activity and job creation. We didn't like it. We don't do that. We don't do that to them, and we don't want them to do that to us. We complained about it and complained about it and called out some of the folks whom we thought were behind this in China.

President Xi visited us in this city about 3 week ago. He and our President had some tough, direct, and probably not entirely comfortable conversations. One of them dealt with this

issue, what we believe is the intrusion by Chinese actors in order to steal our intellectual seed corn, in order to maybe have a short step, a shortcut to economic development, economic activity. They would not have to spend the money, the time, and the energy to do all the research that would lead to this innovation and job-creation activity. The agreement that came out of that was the Chinese and our country have agreed that neither side will knowingly steal this kind of information from the other. ''Knowingly'' is a very broad term, and so we have to make sure that ''knowingly'' actually means something. Secretary Jeh Johnson, the head of the Homeland Security Department, and Attorney General Loretta Lynch have been assigned to build on this initial agreement and see what we can make of it.

I will close with this. A lot of people in our country don't understand what all this cyber security stuff is—intrusion, EINSTEIN, and all the items we are talking about that are in the legislation which is before us this week. They do know this: It is not good when people can steal the kind of information that needs to be protected. Whether it is part of the government domain, military or intelligence secrets; whether it is economic secrets or developments that lead to economic gain; whether it is personally identifiable information that can be used for blackmail purposes or to monetize and to somehow make money off of that information, we know it is not good. There is no one silver bullet to actually stop this kind of activity, but there are a lot of silver BBs, and some of them are pretty big.

The legislation that is before us today, bolstered by similar legislation that has come out of the Committee on Homeland Security and Governmental Affairs, is a pretty good-sized BB. They are not going to enable us to win this war by themselves, but they will enable us to make real progress. It will make us feel a good bit more secure than we have, knowing that this is an enemy across the globe and that a number of enemies wish us harm. They are not going to give up. There is a lot of money involved. They will be back at us, and we have to bring our ''A'' game to work every day in the Department of Homeland Security and other Federal agencies working in tandem with the private sector.

Hopefully, with this information, the folks in the private sector—if they want to get the liability protection and share information with the Federal Government, we want them to use the portal through the Department of Homeland Security. The Department of Homeland Security, to the extent that privacy scrub is needed—it does not happen often. It happens less than 1 percent of the time with the information that comes through the portal. The legislation before us, with the amendments that are offered, will enable us to have that kind of security about our private information and at the same time to do a very good job—a much better job—in protecting what is valuable to us.

Mr. President, I think that is about it for me. I appreciate very much the opportunity to speak. I appreciate the patience of Senator KING, and I will yield the floor to him.

I will just say in closing—no, Senator BLUNT, I will yield to you next. It is good to be with both of you. I look forward to working with you on these and, with respect to the Senator gentleman from Missouri, very closely on related matters.

Thank you so very much.

The PRESIDING OFFICER. The Senator from Missouri.

Mr. BLUNT. Mr. President, I thank the Senator from Delaware. He and I have worked on legislation together to protect data security, to have one standard for notifying people whose information has been accessed by people who shouldn't have it, and we are going to continue to work on that and look for opportunities, whether it is this bill or some other bill, to add that important element to what we are doing here.

I come to the floor today, as I am sure many others have, to express support for this bill—for the Cybersecurity Information Sharing Act—a bill that gives us tools we don't currently have, and to break down barriers that we do currently have. This is a bill that would allow individuals who see the information they are responsible for being attacked to call others in their same business and say: Here is what is happening to us right now. If you are not seeing it already, you should be looking for it. When they do that, it doesn't violate any competitive sharing of information. What it does is bring everybody into the loop of defense as quickly as possible and allow them to look for help from the government as well.

So I express support for this bill. We know that day after day Americans who read, watch, or listen to the news learn of another cyber attack. Some involve attacks of government systems, while others involve the private sector.

In 2012 and 2013, hacker groups linked to Iran targeted American bank Web sites and sustained an attack on those Web sites in a way that was designed to disrupt people trying to do business—trying to pay their own personal bills, trying to do things people should expect to be able to easily do.

Early in 2014, we learned that cyber criminals had stolen 40 million credit card numbers from a major retailer and had probably compromised an additional 70 million accounts. We also have learned that a lot of times when we hear about these, they seem bad enough at first, but they seem a whole lot worse later when we find out what really happened, when we see how deep these criminals were able to go, how deep these terrorists were able to go, how deep these government-sponsored entities were able to go to get at information they shouldn't have.

In September of that same year, September 2014, we learned another major retailer had suffered a data breach. In that case there were 56 million credit card holders.

In February of this year, we learned a health insurance provider's system had been hacked, and 80 million customers were affected. This was a data breach that particularly impacted my State—particularly impacted Missourians—and we saw a huge change in the IRS fraud that occurred this year because, we believe at least, because criminals suddenly had all this sensitive personally identifiable information they had stolen. Suddenly somebody besides you was filing your tax return. Only later did the people who really had the income tax return to file find out that somebody had filed it for them.

In June of this year—maybe the most surprising to all of us who have heard over and over again that the private sector is struggling, we suddenly found out the U.S. Office of Personnel Management increased a previous estimate of how many people were affected by its own data breach. The files of Federal employees and people related to those files was revised upward to 21.5 million people. Then we found out that also included roughly 5.5 million sets of fingerprints.

I am not exactly sure what you could do with somebody's fingerprints on the Internet today. I can only imagine what you might be able to figure out to do with those fingerprints. Remember, your fingerprints don't change, and probably the government entity responsible for that hacking that has those fingerprints is always going to have those fingerprints as they think of new and malicious ways to use them. So we are talking about well over 100 million Americans who already have their personal information in the hands of people it shouldn't be in.

The challenge before us is as clear as it is urgent. Virtually every aspect of our society and our economy rely on information technology. It has enabled tremendous economic growth, it has enabled tremendous efficiencies in every sector, but it has put all kinds of information out there in ways that, looking back, we are going to wonder why we made that information so available in so many places and left so unprotected.

Federal, State, and local governments rely on that information technology as well. As the technology advances, its widespread adoption has also opened us to new dangers. Modern cyber security threats are sophisticated, they are massive, and they are persistent. This doesn't just happen every day, it happens all the time every day.

The culprits of these attacks and intrusions range in terms of their motives and their abilities. We just heard of a teenager who figured out how to

get into the personal account of the CIA director—at least that is the public media report—and the homeland security director. This is not a particularly sophisticated individual, but obviously a pretty capable person who gets to two individuals that one would think would be the most cautious.

Some of these people are bent on sheer vandalism—just the thrill of cyber vandalism—while others are determined to steal intellectual properties from American companies. The motive there is clear. It is easier to steal intellectual property than it is to go through the hard work of creating it. Suddenly that information is out there, and the people who created it have been robbed.

I hear this all the time when I visit companies in my State. We have seen cyber intrusions used for espionage. We have seen one major company attacked for no reason other than to embarrass the company because a foreign government didn't like something the company had done. It is quite a way to have a movie review, that we are just going to destroy as much of your technology as we can by a cyber invasion.

A great many more of these people are motivated by greed—pilfering other people's identities, getting access to other people's account information, and selling that information on the black-market. This becomes a real opportunity for them. The more you remove it from the person who initially got it, the harder it is to find out who initially got it and what they did with it.

Underneath all this is the implication of more serious attacks that can cause physical harm and can cause mass disruption of critical infrastructure of the country that is very dependent on cyber security. This really begs the question: What are we doing to protect our country and our citizens from these cyber adversaries? I have been in Senate for 5 years. I have had the great opportunity to represent the people of Missouri here for 5 years. And during every one of those 5 years, we have been talking about how important it is that we do something about cyber security. This is the only approach I have seen in those 5 years that has bipartisan support. It has a bicameral consensus. This is something that can happen.

This is a problem that it is time to stop talking about. Do we want some other government to have everybody's fingerprints before we do something about it? This is the time to do something about it. As a member of the Senate Select Committee on Intelligence, I am certainly here to support the chairman of that committee and the vice chairman of that committee to finally pass this bill, a bill to enhance the public-private partnerships that can provide the kind of cyber defense we need.

We need to do that and we need to encourage lots of sharing. We need to encourage sharing of attacks. We need to encourage early on, as I said, the ability to call somebody else in your same business and to contact them and say: This is happening right now. That is the best time to say it. The other option is to say: This happened to us late last night or happened yesterday, but this is happening to us. Is it happening to you?

There is lots of misunderstanding about this concept. Without getting too technical, cyber threats are the malicious codes and algorithms used to infect computer systems and attack networks. They are techniques that use bits and bytes. They are the ones and zeros of the digital age that allow hackers to intrude upon private systems, steal information, perpetrate fraud, or disrupt activities over the Internet.

In very dangerous circumstances, these techniques can be used to remotely control critical infrastructure management systems, such as supervisory control and data acquisition systems. I saw something on the news the other day where some hackers, for no intent other than maybe just to see if they could do it, had figured out how to take over one of the cars that was driving itself. Suddenly the car wasn't driving itself; the hacker was driving the car.

When a particular company finds itself subjected to some novel new approach, the quicker they can share that, the better. When the government discovers a new method being used to infiltrate information technology systems abroad or here, they need to be able to share that with American companies quickly so they can protect themselves. There are things the private sector sees that the government does not, and there are things the government sees that the private sector does not. This legislation gives the obligation and opportunity to both of them to join together in this important fight. Modern communications networks move at an incredibly rapid pace. We need to be fighting back at that same kind of rapid pace.

This bill establishes a strictly voluntary program. Unlike some of the other programs we have talked about to secure ourselves in a post-9/11 world, this is a strictly voluntary program that leverages American ingenuity to unleash the arsenal of democracy against cyber adversaries.

When it comes to the cyber threat, we have to act for a common purpose. Throughout this debate there has been a great deal of discussion about the need to protect liberty in the information age. I truly think liberty and security are not at odds with one another in this legislation. When it comes to this bill, it comes the closest to having the balance we all would like to see. It takes into consideration the importance of liberty, but it also takes into consideration what happens as we protect our security.

I would close by saying of all the attacks we have had, and as bad as they have been, none of them have been the sort of catastrophic infrastructure attack that we may see that would impact the grid, that impacts our ability to communicate, impacts our ability to make the water system work, or impacts our ability to make the electrical system work. If that happens, the Congress will not only act, the Congress will overreact.

This is the right time to have this debate. Let's put this legislation on the books right now. Let's give the people a law that makes sense at a time when we have the time to debate it, instead of waiting to see the direction we will turn to when we should have debated this and moved in this direction right now. I encourage my colleagues to vote for this bipartisan bill that I think will wind up on the President's desk and become law.

Mr. President, I yield to my patient friend from Maine, who has been waiting. He and I serve on the Select Committee on Intelligence together, and I look forward to his comments.

The PRESIDING OFFICER (Mr. SCOTT). The Senator from Maine.

Mr. KING. Mr. President, the United States is under attack. We are under attack—not a week ago, a month ago, September 11 or yesterday, but right at this moment. We are under attack from state actors, from terrorist nonstate actors, and from garden-variety criminals. This cyber issue is one of the most serious that we face.

When I first got here, I was appointed to the Armed Services and Intelligence Committees. On those two committees over the past 3 years, at least half of our hearings have touched upon this issue and the threat that it presents to this country. The leaders of our intelligence community and our military community, in open session and in closed session, have sounded the alarm over and over and over. The most dramatic—I don't remember what the hearing was—was when one of our witnesses said: ''The next Pearl Harbor will be cyber.''

As the Senator from Missouri just pointed out, we are fortunate that we have had a number of warning shots but none have been devastating. But we have had warning shots—at Sony, at Target, at Anthem, at the Office of Personnel Management of the U.S. Government, and at the home email of the Director of the CIA. We have had large and small intrusions and cyber attacks that have been more than annoying, but, so far, they haven't been catastrophic. That is just a matter of time. That is why we have to move this bill.

This bill isn't a comprehensive answer to this question, but it is at least a piece of it. It is a beginning. We are going to have to talk about other aspects of our cyber strategy, but at least we can pass this bill, which came out of the committee 14 to 1. It is bipartisan, and it has support in the House. Let's do something.

I do not want to go home to Maine and try to explain to my constituents,

when the natural gas system or the electric system is brought down, that we couldn't quite get around to it because of the difference of committee jurisdictions or because we had other priorities or because we were tied up on the budget. This is a priority. It is something we should be doing immediately, and I am delighted that we have moved to it.

Now, as I have sat in the Intelligence Committee every Tuesday and Thursday afternoon for the past 3 years, it occurred to me several months into those debates and the discussions of this and other issues that really we in the Intelligence Committee and also we in this body really are working with and weighing and balancing two constitutional provisions.

The first is the preamble of the Constitution. The most basic responsibility of any government, anywhere, anytime, is to provide for the common defense. That is why governments are formed, to provide the security, and also to insure domestic tranquility. Those two together are the basic functions of why we are here—to protect our people from harm. And that is clearly what this bill is talking about.

But the other constitutional provision in the picture that we also have to weigh is the Fourth Amendment: ''The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated. . . . '' That is a fundamental premise of who we are as a people.

These two provisions of the Constitution are intentioned—neither one dominates, neither one controls the other—and it is our job in this body to continuously weigh and calibrate these two provisions and their balance in light of threats and evolving technologies.

When the Fourth Amendment was written, nobody had ever heard of telephones. They certainly had never heard of the Internet. They never thought about any of these things. But they said: The rights ''shall not be violated.'' It is interesting—''unreasonable searches and seizures.'' They didn't know the threats we would be facing when they said it was a fundamental premise of the U.S. Constitution that we should protect against both foreign and domestic enemies. That is what we have to do, and that is what this bill does.

This bill is very carefully worked up, with a lot of discussion and negotiation, to be effective in protecting the public, while, at the same time, to be effective in protecting the public's privacy rights in respecting these two principles. We have had warning after warning after warning, and now it is time for us to act.

The good news about the United States is that we are the most wired nation in the world. Technology has been a huge boon to our economy and to our people, and we are way ahead of a lot of the rest of the world in our interrelationship with technology and how we have used it to enhance our lives. That is the good news. The bad news is that we are the most wired country in the world, because that means we are the most vulnerable—asymmetric vulnerability. We are more vulnerable because we are more connected. That means we have to take great care in this country to be sure that we don't allow that vulnerability to result in a catastrophic loss for our people.

Not only are we talking about national security issues, but we are talking about individual people's lives. If the electric grid went down, people's lives would and could be lost—in hospitals, at traffic intersections, across the country. If the natural gas system—the vast pipeline system that links our country in terms of energy—somehow went awry because of a cyber intrusion into the operating system, that would have devastating consequences for human lives and also, of course, for the economy of our country. Somebody could get into the routing system of a railroad, and a train carrying hazardous material would be caused to derail. These are the kinds of things that can happen and will likely happen unless we take steps to protect ourselves.

Some of these attacks and intrusions are sponsored by nation-states. We know that. Some of them are sponsored by just garden-variety criminals who are trying to steal our money. Or some of them are large international criminal organizations that are trying to steal our commercial intelligence and how we build our products and how we compete. Some of them are terrorist organizations that see this as a cheap way to attack America. Why go to all the trouble to build a bomb and smuggle it into the country and all the risk that entails, when you can disrupt the country in just as great a way with a few strokes on a laptop?

It is economic security, national security, economics. It has been estimated worldwide that cyber crime costs our country $445 billion a year. That is to the global economy—a half trillion dollars a year. Some 200,000 jobs in the United States could be and are being affected, and 800 million personnel records were stolen, and 40 million were Americans.

The cost of cyber crime is estimated to be between 15 and 20 percent of the value created by the Internet. We always talk that we don't want any taxes on the Internet. This is a tax. This is a tax we are all paying. The users of the Internet are paying to ward off this epidemic of cyber crime.

It is not only the government. Of course, it is companies, such as Sony, Target, Anthem, the industrial base, JP Morgan, Home Depot. The list goes on and on. Most importantly, it is not just the big guys. Sometimes we feel that OK, this is the large banks, the large insurance companies that have to worry about this. In the State of Maine, we have to worry about it.

My staff and I in Maine have reached out to businesses large and small across the State. Every single one, with one exception, listed cyber intrusion as one of their greatest issues.

The Maine Credit Union League, with $2.5 million a year, and local credit unions are having to deal with cyber intrusion.

One of our Maine health care providers has experienced thousands of attempts to steal confidential data every year. Keeping the data safe is costing them more than $1 million. This is costing us real money.

At one of our Maine financial institutions, 60 to 70 percent of the emails they get in the bank are phishing emails trying to compromise their secured data.

One of our utilities spent over $1 million a year just on preventative costs to defend against cyber crime. This is in a State of 1.3 million people. This is real. This is real in our State.

I had a forum over the August break with businesses throughout Maine—mostly small businesses and homeland security. We had 100 businesses come just to visit and sit for a day to talk about this issue. These were small businesses, and all of them were seeing these kinds of problems.

One was a small business with 35 employees that did a deal overseas, and a cyber criminal in effect stole their payment. They sent a fake invoice to the customer overseas, the customer paid it, and the money went to the crook, not to my company in Maine. That is the kind of thing that is happening, and that is one of the reasons we have to take action today.

No business is immune. No individual is immune. And, of course, this country is not immune.

The price of inaction is just too high. This is something we must attend to. As I mentioned, this bill is not the whole answer, but it is a part of the answer.

Some people say: Well, it is not broad enough. My answer is this: OK, I understand that, but let's do what we can do and then take it one step at a time.

Some people say it compromises privacy. I don't believe that it does. Extraordinary measures were imported into this bill in order to protect the privacy of individuals. This is not about individual data. This is about a company voluntarily telling the government and perhaps some other companies: Here is what I am seeing as an attack. How can we collectively defend ourselves against it?

That is what this bill is really all about. We have to take action, and now is the time.

I thank the chair and the vice chair of the Intelligence Committee, the members of the Homeland Security and Governmental Affairs Committee, the members of the Judiciary Committee, and all of those who have contributed to the finalization of this important piece of legislation.

There is an attitude out there that we can't get anything done around

here. I think this gives us an opportunity to prove that idea wrong. We can get things done. We should get things done. This is a chance for us to protect our people, to provide for the common defense—which is our most solemn constitutional responsibility—in a way that also protects the interests of the Fourth Amendment and individual privacy rights.

I hope we can move swiftly, complete the consideration of this bill this week, work out our differences with the House, and get this matter to the President. We have no place to hide if we don't get this done. This is what we are here for.

Again, I thank my colleagues who worked so hard to bring us to this point.

I yield the floor.

The PRESIDING OFFICER. The Senator from Arizona.

Mr. MCCAIN. Mr. President, before the Senator leaves the floor, I wish to thank him on a well-planned, well-thought-out, and very convincing presentation, and an argument that, frankly, I can add very little to. So I will make my remarks very brief.

I thank the Senator from Maine for highlighting the absolute importance of the passage of this legislation. And, I might add, he is one of the most serious and hard-working members of the Senate Armed Services Committee as well. I won't go any further.

Mr. President, I rise in strong support of S. 754. I thank my colleagues, Chairman BURR and Vice Chairman FEINSTEIN, for their ongoing leadership.

In the short 2 months since this bill was last on the Senate floor, the need for action on information sharing has only increased. It is not for a lack of trying. We have continuously failed to make progress on this bill. As the Senator from Maine just made clear, that must change. Enacting legislation to confront the accumulating dangers of cyber threats must be among the highest national security priorities of the Congress.

The need for congressional action, in my view, is also enhanced by the administration's inability to develop the policies and framework necessary to deter our adversaries in cyberspace.

Earlier this week we learned just how ineffective the administration has been in addressing our cyber challenges. Within days of reaching an agreement to curb the stealing of information for economic gain, China—China—repeatedly, reportedly, continues its well-coordinated efforts to steal designs of our critical weapons systems and to wage economic espionage against U.S. companies. It is not a surprise, but it serves as yet another sad chapter in this administration's inability to address the cyber threats.

I guess in the last couple of days it has been made known that some hacker hacked into the information of both the Director of the CIA and the chairman of the homeland security committee. That is interesting. As the President's failed China agreement clearly demonstrates, our response to cyber attacks has been tepid at best and nonexistent at worst. Unless and until the President uses the authority he has to defer, deter, defend, and respond to the growing number in severity of cyber threats, we will risk not just more of the same but embolden adversaries in terrorist organizations that will continuously pursue more severe and destructive attacks.

Addressing our cyber vulnerabilities must be a national security priority. Just this week, Admiral Rogers, the head of Cyber Command, reiterated, ''It's only a matter of time before someone uses cyber as a tool to do damage to critical infrastructure.''

My colleagues don't have to agree with the Senator from Maine or me or anybody else, but shouldn't we listen to Admiral Rogers, the head of Cyber Command, probably the most knowledgeable person or one of the most knowledgeable who said, ''It is only a matter of time before someone uses cyber as a tool to do damage to critical infrastructure.''

According to the recently retired Chairman of the Joint Chiefs of Staff, General Martin Dempsey, our military enjoys ''a significant military advantage'' in every domain except for one—cyber space. As General Dempsey said, cyber ''is a level playing field. And that makes this chairman very uncomfortable.''

I will tell you, it makes this chairman very uncomfortable as well.

Efforts are under way to begin addressing some of our strategic shortfalls in cyber space, including the training of a 6,200-person cyber force. However, these efforts will be meaningless unless we make the tough policy decisions to establish meaningful cyber deterrence. The President must take steps now to demonstrate to our adversaries that the United States takes cyber attacks seriously and is prepared to respond.

This legislation is one piece of that overall deterrence strategy, and it is long past time that Congress move forward on information sharing legislation. We have been debating similar cyber legislation since at least 2012. I am glad this body has come a long way since that time in recognizing that government mandates on the private sector, which operates the majority of our country's critical infrastructure, will do more harm than good in cyber space. The voluntary framework in this legislation properly defines the role of the private sector and the role of the government in sharing threat information, defending networks, and deterring cyber attacks.

At the same time, it is unfortunate that it has taken over 3 years to advance this commonsense legislation. The threats we face in cyber space are real and imminent, as well as quickly evolving. All aspects of the Federal Government, including this body, must commit to more quickly identifying, enacting, and executing solutions to counter cyber threats. If we do not, we will lose in cyber space.

As chairman of the Armed Services Committee, I consider cyber security one of the committee's top priorities. That is why the National Defense Authorization Act provides a number of critical authorities to ensure that the Department of Defense can develop the capabilities it needs to deter aggression, defend our national security interests, and when called upon, defeat our adversaries in cyber space. I find it unacceptable that the President has signaled his intent to veto this legislation that, among other key Department of Defense priorities, authorizes military cyber operations and dramatically reforms the broken acquisition system that has inhibited the development and delivery of key cyber capabilities.

More specifically, the National Defense Authorization Act extends liability protections to Department of Defense contractors who report on cyber incidents or penetrations, and it authorizes the Secretary of Defense to develop, prepare, coordinate and, when authorized by the President, conduct a military cyber operation in response to malicious cyber activity carried out against the United States or a U.S. person by a foreign power. The NDAA authorizes $200 million for the Secretary of Defense to assess the cyber vulnerabilities of every major DOD weapons system. Finally, Congress required the President to submit an integrated policy to deter adversaries in cyber space in the fiscal year 2014 National Defense Authorization Act. I tell my colleagues that we are still waiting on that policy. This year's NDAA includes funding restrictions that will remain in place until it is delivered.

As we dither, our Nation grows more vulnerable, our privacy and security are at greater risk, and our adversaries are further emboldened. The stakes are high, and it is essential that we pass the Cybersecurity Information Sharing Act without further delay.

Let me also mention in closing that probably the most disturbing comment I have heard in a long time on this issue in this challenge is when Admiral Rogers said that our biggest challenge is we don't know what we don't know. We don't know what the penetrations have been, what the attacks have been, whether they have succeeded or not, where they are in this whole realm of cyber and information at all levels. When the person we placed in charge of cyber security says we don't know what we don't know, my friends, that is a very serious situation.

I want to congratulate again both the managers of the bill in their coordination and their cooperation in this bipartisan effort.

I yield the floor.

Mr. KING. Will the Senator yield for a question?

Mr. MCCAIN. I will be pleased to yield.

Mr. KING. I ask the Senator, would you agree that this bill represents an important part of our cyber defense but that in order to deter attacks in the long term, we must have a cyber policy that goes beyond simple defensive measures?

Mr. MCCAIN. I would certainly agree, I would say to my friend from Maine, because if the adversaries that want to commit cyber attacks against the United States of America and our allies believe that there is no price to pay for those attacks, then where is the demotivating factor in all of this which would, if they failed, then keep them from doing what they are doing? It seems to me that this is an act of war, and I don't use that term lightly but I am trying to use it carefully. If you damage intentionally another nation's military or its economy or its ability to function as a government—I would ask my friend from Maine—wouldn't that fit into at least a narrow interpretation of an act of war? If so, then should we only have defenses? Have we ever been in a conflict where we only have defenses and not the capability to go out and deter further aggression?

Mr. KING. I would suggest to the Senator that if you are in a fight and all you can do is defend and never punch, you are going to eventually lose that fight. I think this is an important area. The theory of deterrence, as distasteful as it might have been, the mutually assured destruction during the nuclear era did in fact prevent the use of nuclear arms for some 70 years. I think we need to be thinking about a deterrence that goes beyond simply defensive measures. I commend the chairman for raising this issue and appreciate your thoughtful consideration.

Mr. President, I yield the floor.

Mr. LEAHY. Mr. President, it seems as though every week, the American people learn of yet another data breach in which Americans' sensitive, private information has been stolen by cyber criminals or foreign governments. This is a critical national security problem that deserves action by Congress. But our actions must be thoughtful and responsible, and we must recognize that strengthening our Nation's cyber security is a complex endeavor with no single solution.

According to security researchers and technologists, the most effective action Congress can take to improve our cyber security is to require better and more comprehensive data security practices. That is why earlier this year, I introduced the Consumer Privacy Protection Act. That bill requires companies to utilize strong data security measures to protect our personal information and to help prevent breaches in the first place. Companies that benefit financially from gathering and analyzing our personal information should be obligated to take meaningful steps to keep it safe.

But rather than taking a comprehensive approach that addresses the multiple facets of cyber security, the Republican majority appears to be focused entirely on passing the Senate Intelligence Committee's cyber security information sharing bill. While legislation to promote the sharing of cyber threat information could, if done right, be useful in improving our cyber security, it is a serious mistake to believe that information sharing alone is the solution. Information sharing alone would not, for example, have prevented the breach at the Office of Personnel Management, nor would it have prevented other major breaches, such as those at Target, Home Depot, Anthem, or Sony.

Instead of ensuring that companies better safeguard Americans' data, this bill goes in the opposite direction, giving large corporations more liability protection and even more leeway on how to use and share our personal information with the government—without adequate privacy protections.

Also troubling is the fact that the Republican majority has been intent on jamming this bill through the Senate without any regard for regular process or opportunity for meaningful public debate. Only last year, the Republican leader declared his commitment to ''a more robust committee process'' and plainly stated that ''bills should go through committee.'' But the bill was drafted behind closed doors by the Senate Intelligence Committee, and it has not been the subject of any open hearings or any meaningful public debate. The text of the bill was only made public after it was reported to the Senate floor, and no other committee of jurisdiction—including the Judiciary Committee—was allowed to consider and improve the bill.

The Judiciary Committee was prevented from considering this bill even though it contains numerous provisions that affect matters squarely within our jurisdiction. First and foremost, the bill creates a framework of information sharing that could severely undermine Americans' privacy. The bill also overrides all existing law to provide broad liability protections for any company that shares information with the government. It also overrides important privacy laws such as the Electronic Communications Privacy Act, ECPA, and the Foreign Intelligence Surveillance Act, FISA, over which the Judiciary Committee has long exercised jurisdiction. CISA even amends the Freedom of Information Act, FOIA, and creates new exemptions from disclosure.

This is just the latest attempt by the majority leader to bypass the Judiciary Committee and jam a bill through the Senate that contains provisions within the jurisdiction of the committee. The bill reported by the Senate Intelligence Committee includes a broad and unnecessary FOIA exemption. FOIA falls under the exclusive jurisdiction of the Senate Judiciary Committee and changes affecting this law should not be enacted without full and careful consideration by the Judiciary Committee. This important transparency law certainly should not be amended in closed session by the Senate Intelligence Committee.

Shortly after the text of the bill was released, I shared with Chairman GRASSLEY my concern that the Judiciary Committee should also consider this bill. He assured me that there would be a ''robust and open amendment process'' if this bill were considered on the Senate floor. But only a few weeks later, the Republican leadership—with Chairman GRASSLEY's support—attempted to jam the Intelligence Committee's bill through the Senate as an amendment to the National Defense Authorization Act, NDAA, without any opportunity for meaningful debate. Republicans and Democrats joined together to reject the majority leader's effort to force the cyber security bill onto the NDAA. Despite this rebuke from both sides of the aisle, just a few weeks later, the majority leader again attempted to jam the bill through the Senate in the final days before August recess, without any serious opportunity to debate and offer amendments.

The majority leader's actions have been part of a consistent disregard for regular order. He has talked about providing an opportunity for fair debate, but at the same time, he has used all procedural mechanisms to stifle process on this bill. Yesterday afternoon, the Senate moved to consideration of this bill—but then not even 2 hours later, the majority leader moved to end debate. That speaks volumes about whether the majority leader is really interested in a full and open debate, and it is not how the U.S. Senate should operate—particularly when it comes to a bill with such sweeping ramifications for Americans' privacy.

Senator FEINSTEIN, the ranking member of the Intelligence Committee, has consistently said that the Senate ''should have an opportunity to fully consider the bill and to receive the input of other committees with jurisdiction in this area.'' She has worked hard to improve the underlying bill with a managers' amendment that addresses a number of my concerns, particularly in regard to FOIA, limiting the sharing of information for cyber security purposes only, and ensuring that the bill would not allow the government to use information to investigate crimes completely unrelated to cyber security. I appreciate these improvements, and Senator FEINSTEIN's efforts to include them in the bill. But again, this bill still has some serious problems and requires a full, public debate. The bill still includes, for example, a FOIA exemption that I believe is overly broad and unnecessary.

In July, the Department of Homeland Security wrote a letter to Senator FRANKEN stating that in their view the bill raises significant operational concerns and certain provisions threaten to severely undermine Americans' privacy. Last week, the Computer & Communications Industry Association—an

organization that includes Google, Facebook, and Yahoo!—voiced serious concerns that the bill fails to protect users' privacy and could ''cause collateral harm'' to ''innocent third parties.'' And this week, major tech companies such as Apple, Dropbox, Twitter, and Yelp have vocally opposed the bill citing concerns for their users' privacy.

The latest version of the bill contains a number of improvements that I and other Senators have been fighting for, and I am glad to see that we are making progress. But we still have work to do on this bill, and the Senate must have an open and honest debate about the Senate Intelligence Committee's bill and its implications for Americans' privacy. I agree that we must do more to protect our cyber security, but we must be responsible in our actions. Legislation of this importance should not be hastily pushed through the Senate, without a full and fair opportunity for Senators to consider the ramifications of this bill. Unfortunately, by moving so quickly to end debate, it appears that the majority leader is trying to do just that.

Ms. MIKULSKI. Mr. President, I wish to support the Cybersecurity Information Sharing Act of 2015.

Cyber security is the most pressing economic and national security threat facing our country today. As a member of the Senate Select Committee on Intelligence, I am keenly aware of the damage cyber attacks cause on our Nation. As vice chairwoman of the Senate Appropriations Committee, I believe we must have a clear and comprehensive approach to funding cyber security.

In boardrooms and around kitchen tables, concern over cyber security is heightening. It is gaining new traction following the cyber attack on the Office of Personnel Management, which compromised the personal information of more than 22 million Federal employees, contractors, and their families.

The American people expect serious action by Congress. This can and must be done, while respecting privacy and avoiding data misuse by the government or businesses. Congress must act with a sense of urgency to pass the Cybersecurity Information Sharing Act. If we wait for another major cyber attack, we risk overreacting, overregulating, overspending, and overlegislating. The time to act is now.

Our Nation is under attack. Every day, cyber attacks are happening. Cyber terrorists are working to damage critical infrastructure by taking over the power grid or disrupting air traffic control. Cyber spies are moving at breakneck speeds to steal state secrets, intellectual property, and personal information. Cyber criminals are hacking our networks, stealing financial information, and disrupting business operations. These cyber attacks can disrupt critical infrastructure, wipe out a family's entire life savings, take down entire companies, and put human lives at risk. In the past year alone, we've seen cyber attacks against Sony, Home Depot, UPS, JP Morgan Chase, Experian, T-Mobile, Scottrade, and the list goes on. The economic losses of cyber crime are stunning. In 2014, the Center for Strategic and International Studies and McAfee estimated the annual cost from cyber crime to be over $400 billion.

I have been working on cyber issues since I was elected to the Senate. Our cyber warriors at the National Security Agency are in Maryland, and I have been working with the NSA to ensure signals intelligence was a national security focus even before cyber was a method of warfare.

In my role on the Intelligence Committee, I served on the Cyber Working Group, which developed findings to guide Congress on getting cyber governance right, protecting civil liberties, and improving the cyber workforce.

As vice chairwoman of the Appropriations Committee and the Commerce, Justice, and Science Subcommittee, I put funds in the Federal checkbook for critical cyber security agencies. These include the Federal Bureau of Investigation, which investigates cyber crime; the National Institute of Standards and Technology, which works with the private sector to develop standards for cyber security technology; and the National Science Foundation, which researches ways to secure our Nation. As a member of the Appropriations Subcommittee on Defense, I fight for critical funding for the intelligence and cyber agencies, including the National Security Agency, Central Intelligence Agency, and Intelligence Advanced Research Projects Activity, who are coming up with the new ideas to create jobs and keep our country safe. These funds are critical to building the workforce and providing the technology and resources to make our cyber security smarter, safer, and more secure.

This bill does three things from a national security perspective. First, it allows businesses and government to voluntarily share information about cyber threats. Second, it requires the Director of National Intelligence to share more cyber threat information with the private sector, both classified and unclassified. Third, it establishes a Department of Homeland Security ''portal'' for cyber info-sharing with the government to help dot-gov and dot-com in a constitutional manner. These three provisions are an innovation. Despite all the amazing talent companies have, many are being attacked and don't even realize it. This legislation allows unprecedented dot-com and dot-gov cooperation. There are also key provisions on privacy protections and liability protection for companies that monitor their own networks or share information.

Why do we need a bill to make these vital partnerships happen? America is under attack every second of every day. The threat is here, and it is now. If we do not act or if we let the perfect be the enemy of the good, this country will be more vulnerable than ever before, and Congress will have done nothing.

This bill is not perfect. The Department of Homeland Security's role has been criticized by many, including myself. I have been skeptical about their ability to perform some duties assigned in this bill. I am still skeptical, although less so than before. But this bill takes important steps to diversify government and private sector actors, so we are not just focusing on DHS, but also keeping civilian agencies in charge. We cannot have intelligence agencies leading this effort with the private sector. Some would like to see that go further, but that is what the amendment process is for.

People in the civil liberties community worry that this bill could allow government intrusions into people's privacy. This was of tantamount concern for me. If we don't protect civil liberties, the added security is for naught because we lose what we value most: our freedom. The authors of this bill, especially Senator FEINSTEIN, have made key improvements on issues of law enforcement powers and protecting core privacy concerns. While not everyone is entirely pleased, this bill has made important strides to balance information sharing and privacy.

The business community is concerned because it fears strangulation and overregulation. They worry that they will open themselves up to lawsuits if they participate in the program with the government. I have heard from Maryland businesses and these are valid concerns. Importantly, this bill has made strides in accommodating business and builds a voluntary framework to allow businesses to choose that protection. Protection does not come without responsibility for participants, but this bill links the need for cyber security, appropriate liability protection, and the expertise of our business community in a way that answers a lot of companies' concerns. We cannot eliminate all government involvement in this issue because it simply won't work, and we will lose key government expertise in the Department of Defense, Federal Bureau of Investigation, and elsewhere. However, we can work to try to minimize it while maintaining the government's role in protecting national security.

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

AMENDMENT NO. 2557

Mr. President, today I wish to speak about my amendment to the cyber security bill. This amendment would provide an additional $37 million for the Office of Personnel Management, OPM,

to accelerate completion of its information technology, IT, modernization and thwart future cyber attacks.

This additional funding would allow OPM to make needed upgrades to cyber security and network systems 1 year ahead of schedule. This means OPM will not have to wait another year to protect sensitive personnel data by implementing hardware and software upgrades recommended by security experts.

The $37 million is designated as an emergency under the Budget Control Act of 2011.

For over a year, the Office of Personnel Management's systems were compromised. This hack exposed the financial and personal information of 22 million Federal employees and their families, contractors, job candidates and retirees. This is unacceptable.

OPM's retirement services and background investigation databases contain the most sensitive data OPM holds, including Social Security numbers, health information and fingerprints.

I have heard from employees across the government. Data breaches undermine morale and complicate their ability to serve the American people.

OPM has moved to provide protections, but that is not enough. Securing these systems must be done now. We can't wait for the next budget cycle.

I urge support for my amendment. This is a crisis, so we ought to treat it like one. Twenty-two million Americans who entrusted their data and fingerprints to the government deserve the highest standard of protection.

There is a reason OPM was exploited. Federal cyber security has been weak. The Appropriations Committee has consistently given agencies the resources they asked for to protect their dot-gov systems. But under sequester-level budgeting it hasn't been enough. Constrained agencies don't ask for what is truly needed to do the cyber security job.

Tight budgets mean immediate problems get requested and funded before other much needed IT protection and maintenance. We aren't even doing the simple things.

After the OPM breach, the Office of Management and Budget, OMB, conducted a cyber sprint. OMB asked agencies to take four minimal steps: No. 1, deploy Department of Homeland Security malicious activity detectors; No. 2, patch critical vulnerabilities; No. 3, tighten privileged user policies; and No. 4, accelerate deployment of multifactor authentication.

While there was improvement, only 14 of the 24 agencies met the fourth goal. Some of it is a lack of will, but some is a lack of resources.

OPM knows it needs to harden its information technology.

That is why I am offering this amendment, providing $37 million in emergency spending to harden OPM systems now—not a year from now. These funds meet the criteria for being designated as emergency spending as set out in the Budget Control Act of 2011. OPM's needs are urgent, temporary, and, regrettably, unforeseen.

What does it mean to designate funds as emergency spending? It means no offsets, so we don't pay for this amendment by drawing from existing funding used to defend the Nation or help America's families.

The need is urgent—our adversaries are still trying to attack us. The need is temporary—these are one-time costs to accelerate IT reform. And the need is unforeseen which is sadly the reason they were not requested in the President's fiscal year 2016 budget in February.

Some say this funding is premature, and OPM is not ready to deploy it effectively. However, those reports were written before Beth Cobert became OPM Acting Director. She is turning OPM around, but she needs the resources to secure OPM's IT systems, and cyber security is a critical issue.

Government can't be reckless with the sensitive data it has. We must do better with dot-gov and get our own house in order. We know what OPM needs to do—they have the will, they have a business plan, and now they need the wallet.

Vote for my amendment No. 2557 to get OPM the resources it needs.

The PRESIDING OFFICER. The Senator from Wisconsin.

UNANIMOUS CONSENT REQUEST—H.R. 3594

Ms. BALDWIN. Mr. President, last week when I was back in my home State of Wisconsin, I had the privilege of hosting a roundtable with college students from all across the southeastern area of the State. The focus of the conversation was how we in Congress could help keep college affordable and accessible. During the course of that conversation, it was abundantly clear that most of the students were very frustrated that Congress could not take some of the most commonsense steps to make that happen. I told them that I shared their frustration and ensured them that I would be going back to Washington, DC, this week to fight on their behalf.

This morning I hosted a Google Hangout and spoke with campus newspapers from across the State of Wisconsin to reiterate my commitment on this issue. So here I am, almost 1 month from the day that I last stood here on the Senate floor, 1 month since a single United States Senator stood up and blocked a commonsense and bipartisan measure that would have continued to provide critical financial support for America's low-income college students.

In the short month since our efforts to reauthorize the Federal Perkins Loan Program were obstructed, the immediate impacts are already becoming quite clear. Last week, the Coalition of Higher Education Assistance Organizations began surveying colleges and universities that participate in the Perkins loan program to learn more about how this obstruction is impacting their students. After a few days, they heard from over 100 students outlining how allowing Perkins to expire is harming students and institutions alike. There are real impacts being felt by real students right now across America. If we don't act, this damaging impact will ripple across our community. Therefore, we cannot sit idly by.

Mr. President, I ask unanimous consent that the Senate proceed to the immediate consideration of H.R. 3594, which is at the desk, that the bill be read a third time and passed, and the motion to reconsider be considered made and laid upon the table with no intervening action or debate.

The PRESIDING OFFICER. Is there objection?

Mr. MCCAIN. Mr. President, on behalf of the leadership, I object.

The PRESIDING OFFICER. Objection is heard.

Ms. BALDWIN. Mr. President, this is incredibly frustrating. I am going to spend a few minutes talking about how this objection, this obstruction is impacting the students of America and the higher education institutions of America. There are real impacts that are being felt right now. Students who have previously received Perkins loans will lose their future eligibility if they change institutions or academic programs. Students seeking Perkins loans for the upcoming winter and spring semesters will not be eligible at all if we don't act soon to reauthorize this program. Finally, all future students will be ineligible for this program.

This afternoon right before I came down to the Senate floor, I received a letter from the president of the University of Wisconsin's system, Ray Cross—a letter that was co-signed by all 14 of the UW system university chancellors. In their message, they shared compelling insight into how the sudden end to the Federal Perkins Loan Program is already affecting Wisconsin students. They then closed their letter with this:

> [W]e need to keep this program in place. After all, our job is to help students who would not otherwise be able to attend higher education and to help them overcome barriers, particularly financial barriers, all of which helps to ensure access, retention, completion, and a skilled workforce. These are goals upon which all of us can agree.

One month ago our colleagues in the House of Representatives—a body rarely called a place of agreement—took up and passed a measure that would extend this student loan program for 1 year. I previously called up that bill here in the Senate and asked unanimous consent that we extend the Federal Perkins Loan Program. While I look forward to a broader conversation about improving Federal supports for students as we look to reauthorize the Higher Education Act, I don't believe—and I still don't—that we can sit idly by while America's students are left with such uncertainty.

As everyone heard, I asked unanimous consent to proceed to the consideration of the bill, and one Senator stood up on behalf of Republican leadership and blocked our ability at this

point in time to extend the Federal Perkins Loan Program by 1 year.

Again, I understand a desire, and frankly, share a desire to have a broader conversation about Federal student aid as part of the Higher Education Act reauthorization effort. I still do not think it is right or fair to let this program expire to the detriment of thousands of students in need. Frankly, this is a perfect example of why the American people are so upset with Washington.

Since 1958, the Federal Perkins Loan Program has been successfully helping Americans access affordable higher education with low-interest loans for students who cannot borrow or afford more expensive private student loans.

In Wisconsin, the program provides more than 20,000 low-income university and college students with more than $41 million in aid, but the impact of this program isn't just isolated to the Badger State. In fact, the Federal Perkins Loan Program aids over half a million students with financial need each year across 1,500 institutions of higher learning.

The schools themselves originate, service, and collect the fixed interest loan rates, and what is more, institutions maintain loans available for future students because these are revolving funds.

Since the program's creation, institutions have invested millions of dollars of their own funds into the program. In addition to making higher education accessible for low-income students, the program serves as an incentive for people who wish to go into public service by offering targeted loan cancellations for specific professions in areas of high need, such as teaching, nursing, and law enforcement.

As a member of the Senate Health, Education, Labor and Pensions Committee, and as a Senator representing a State with such a rich history of higher education, it is among my highest priorities to fight to ensure that the Federal Perkins Loan Program continues for generations to come, but unfortunately, as we saw, one single Senator stood up again today and said no to students across America who ask for nothing more than an opportunity to pursue their dreams—students such as Andrew.

Andrew is currently a student at the University of Wisconsin in Stevens Point. Without the support of his Perkins loan, Andrew said he would not have had the means to attend college. He has little to no income at his disposal. Today, not only is Andrew making the dean's list every semester, but he now has his sights set on attending law school, also at the University of Wisconsin. Andrew said: ''Without the assistance I get from the Perkins Loan I would be forced to either take out other high-interest loans, or delay my graduation date, or drop out—which is the last thing I want to do.''

Today this body also stood up and once again said no to students such as Nayeli Spahr. Nayeli was raised by a single mother who was an immigrant and worked two full-time jobs. Nayeli attended 10 different schools in 3 different States before she finished high school. Without the Federal Perkins Loan Program, Nayeli said her opportunity to get a college education would have been ''an illusionary dream.''

Today Nayeli is the first in her family to finish college and is now in her last year of medical school. She is planning to work with those who are underserved in our urban communities. She finished by saying:

> The Perkins loan program helped me reach this point. And its existence is essential to provide that opportunity for other young adults wanting to believe in themselves and to empower their communities to be better. Please save it!

You don't have to look very far to find the dramatic impact that this investment has on America's students. There are thousands of stories like the ones I just shared, representing thousands of students who are still benefitting from the opportunities provided to them by this hugely successful program.

I am disappointed and frustrated that our bipartisan effort in the Senate has again been obstructed. I will continue to fight to extend support for America's students in the form of extending the Federal Perkins Loan Program so that we can find a way to show the half-million American students who rely on this loan program that we are standing with them and that we are committed to helping them build a stronger future for themselves and our country.

I thank the Presiding Officer, and yield back the remainder of my time.

The PRESIDING OFFICER (Mr. GARDNER). The Senator from Ohio.

Mr. PORTMAN. Mr. President, I join my colleague from Wisconsin and other Members who are here on the floor to talk about the Perkins Loan Program. It is a really important program. It serves the needs of many of the students in our States, and it serves a unique need. It provides flexibility that other programs don't provide, and it also allows the colleges and universities to actually contribute to it.

I hope we can get this 1-year extension done, and I hope that the objection will be overridden by the common sense of doing something that the House has already done. By the way, the House of Representatives did it for 1 year also at no cost to the Federal Government because there is no reason to pay for a 1-year extension of a program that is a loan program where the colleges and universities take the payments that are made—the repayments—and put them back into the program. So this program is at no cost, and it is certainly an important program that we ought to continue.

I know there is discussion about broader education reform, and I support that. I know this program is not perfect. There are other ways that we could possibly improve it. I am perfectly willing to enter into that discussion and debate it. We should have that debate. We should debate how to make sure college is more affordable for all students, but let's not at this point stop this program that is working and is providing for young people in my State and around the country what they need to be able to afford a quality education.

I was out here a few weeks ago talking about this program, and at that time I talked about some specific schools and the people in my State who depend on this program. It is the oldest Federal program out there that allows students to be able to take advantage of some kind of help in order to get through school, and boy, it is needed now more than ever with tuition costs going up and more and more families feeling the squeeze.

When I go back home, I hear from parents and the students themselves. It is tough. Wages are flat, and in many cases declining. Yet expenses are up, and this is one of them, along with health care and electricity bills. This is not the time to stop the program but to continue this really important program. At the same time, we need to engage in the important debate of how we can reform higher education more generally in order to ensure that everybody has access to an affordable education.

Since 1958, this program has provided more than $28 billion in loans. It is a program that supports 60 different schools in my State. In the Buckeye State of Ohio, we have 60 schools that have loans under this program. Last year, more than 25,000 Ohio students received financial aid through this program—3,000 young people at Kent State and over 1,700 at the Ohio State University in Columbus.

One of those students is an outstanding young woman. Her name is Keri. She is a junior at Kent State. She interned for me last summer. When I talked to Keri about this program, she said that this is something she absolutely needs to be able to stay in school.

Keri is a young woman for whom I have a lot of respect because she fought the odds. She was in foster care. She went from one foster home to another while she was growing up. Yet she not only fought the odds. She is now excelling in college and doing a great job, but she doesn't have the resources to stay in college without this program. She is a Pell grant recipient, but she also needs the Perkins Loan Program to be able stay in school.

This is not just about numbers, folks. This is about people. This is about Keri. This is about young people whom we want to be able to have the opportunity and to be able to get the education they need to get ahead, because it does provide help for those who are most in need.

Well beyond Ohio, of course, 1,700 postsecondary institutions now participate in this program. It shouldn't be

controversial. Again, the House passed it for 1 year. It is something that does not require a new appropriation. It is a flexible program. So many of our student loan programs, including the Pell Grant Program and so on, are programs where the schools cannot provide any kind of flexibility. With many of our families and many of our students, Keri being an example, that flexibility is really important. Circumstances change. They may find themselves in a situation where they need a little help to stay in school so they can finish their academic major. They may find they need a little bit of help because of an unfortunate event that they could not anticipate happening in their families, and this program provides that flexibility. Again, the colleges and universities actually contribute to it. It is a matching program where they have to step up and be counted.

Let's not allow these students to fall through the cracks, and let's consider what happens if we do allow that to happen. Students who are applying for the winter semester, which starts in January, or the spring semester may well find that they are not able to receive the aid they need.

I am told that students can lose their eligibility if they change institutions or if they change their majors. These kids could fall between the cracks even if they have a Perkins loan now.

Finally, of course, if we don't act pretty soon, then next fall when there will be up to 150,000 freshman looking for a Perkins loan, they may find they are not eligible for it. This is not acceptable. Let's be sure we do everything we can here to make sure that college is not road-blocked for low-income students who are trying to get a college degree and pursue their dreams. Let's help them get ahead.

Let's pass this. It creates certainty for the students who benefit from the loans, it creates certainty for these colleges and universities, and it ensures that students who need this funding are not stopped and blocked by these high tuitions.

I wish to thank my colleagues Senator COLLINS and Senator CASEY, whom I see is on the floor. I also wish to thank Senator BALDWIN, Senator AYOTTE, Senator MURPHY, and I see Senator COONS and others who are here.

This is bipartisan, and it is something we can do here in the Senate, just as the House has already acted. Let's not block this program because this could block the students from attaining the educational background they need to be able to succeed in life. Let's move forward with this while at the same time continuing our discussion on the need to ensure that higher education is more broadly reformed to allow everybody to have that opportunity to pursue their dreams.

I thank the Presiding Officer, and I yield my time.

The PRESIDING OFFICER. The Senator from Connecticut.

Mr. MURPHY. Mr. President, let me associate myself with the remarks of Senator BALDWIN and Senator PORTMAN. I thank them for making this bipartisan clarion call to bring this body together on behalf of students. There are over 6,000 students in my State of Connecticut.

I believe Senator BLUMENTHAL is going to give some remarks as well to add Connecticut's list of schools and to debate this issue on the floor.

We have over 1,000 students at the University of Connecticut, over 700 at Yale University, 600 at the University of Bridgeport, 500 at Central Connecticut, and 400 in Eastern Connecticut. All across Connecticut, students are able to attend college because of the Perkins Loan Program. As one of the few Members of the Senate who is still paying back my student loans, who is also saving as fast as I can for my two boys who will hopefully go to college, this debate we are having today strikes me as crazy. We should be having a debate about how we expand access to college. Instead, we are simply trying to protect the existing access we have.

In 10 years the United States has gone from the No. 1 country in the world with respect to the number of 25- to 35-year-olds with college degrees to number 12 in the world. In 10 years we have gone from first to twelfth. The answer for that is the cost of college. The cost of college is making it unaffordable for people to start and unaffordable for many others to complete it.

The Perkins Loan Program is one that doesn't require any additional expenditure of taxpayer dollars. Those 6,000 kids in Connecticut will get to continue to attend college with Perkins loans, with no additional obligation on behalf of taxpayers. That is as good a deal as we can get—no additional expenditure from the Federal Government and hundreds of thousands of kids all across the country—6,000 of them in Connecticut—get to continue in college.

I simply wanted to come to the floor to express my bewilderment that the Republican leadership is standing in the way of simply preserving the student loan programs that are on the books today. If we go back home to our districts, we are not going to hear from a lot of people who are sympathetic to this argument. They want Congress to be talking about how to make college more affordable. They would be as bewildered as many of us are that Republicans in the Senate are trying to make college less affordable, when there is absolutely no additional expenditure required in order for us simply to preserve the Perkins Loan Program as it currently exists.

Let me just add one story to the mix—the story of Amanda, who is a senior at the University of Hartford. Her family makes about $67,000 a year. People are going to be familiar with her story because that is just a little bit too much for her to be able to qualify for a Pell grant. So she has to work two different jobs to put money on top of her Stafford loans, to put money on top of the contribution her parents make, just to get into the neighborhood of being able to afford college, but what makes that final difference for Amanda is the Perkins loan.

The only reason she is able to go to the University of Hartford is because of the Perkins loan. She is doing everything we ask. Her parents are putting in some money, she is taking out loans, and she is working two jobs. She says:

> I can't imagine how difficult it would have been if federal funding sources such as the Perkins loan had been eliminated as options for me. I've utilized the Perkins loan offered to me, in the full amount, every single year to resolve my account balance. Even now, in my senior year, I have no choice but to work two jobs and I'm barely getting by. Without the Perkins and other financial aid, I truly believe that I would have had to transfer to a community college where I would not have been able to accomplish nearly as much as I have here at the University of Hartford.

On behalf of her and the six other students in Connecticut who will lose their Perkins loan eligibility as long as this Republican objection lasts, I hope it will come together.

Thank you, Mr. President.

I yield the floor.

The PRESIDING OFFICER. The Senator from Delaware.

Mr. COONS. Mr. President, I stand to join in with the voices we have already heard from, including Senator MURPHY of Connecticut and Senator PORTMAN of Ohio—bipartisan, of course—who have stood in support of the unanimous consent request of Senator BALDWIN, blocked by the opposing party, that we move forward with reauthorizing the Perkins Loan Program.

The voice that I think is so often missing from the deliberations in the Senate is the voice we just heard brought forward by Senator MURPHY of Connecticut, the voice of our constituents—the constituents who connect with us when we are home in our States; the constituents who reach out to us by letter and by email. I just wanted to add the voices of my constituents from the State of Delaware.

Apparently, our colleagues have failed to hear from thousands—even hundreds of thousands—of our home State constituents who rely on Federal Perkins loans. This program is a critical lifeline for students across the country who would be well on their way to a college degree if it weren't for the skyrocketing, unsustainable costs of higher education. I think Congress's failure to reauthorize the Perkins Loan Program is already having a negative impact on students and on households across our country. We can see the real-world impact in our home States if we will but listen to our constituents.

Let me give two examples of Delawareans who have recently reached out to me.

Frank, an incoming University of Delaware student, was counting on the

Perkins Loan Program to help cover a gap in affording the cost of his higher education. Now that those funds are no longer available, now that the Perkins loans have expired, his family is struggling to figure out how they will pay for his education.

There is also Taylor, a Delawarean, already a college student, who had signed up for a promising new course of study because of a Perkins loan that would make the additional cost possible. Without this funding moving forward, future students like Taylor will also have to turn to private loans—sometimes less accessible, sometimes less affordable—to fill that gap. Frank and Taylor's stories are just a few examples of many that I have received in my office from constituents or conversations I have had at home in Delaware.

When I am with working Delawareans, there is no topic raised more frequently amongst those in my age bracket of how they can afford to send their kids to college. Just the other night, standing around on the sideline of a soccer game, I heard a whole group talking about how can we possibly afford the skyrocketing expenses of higher education.

So the question we are here today to address isn't the great big question of how can we make college affordable, it is just a simple question of how can we extend the Perkins Loan Program. I am proud to join with my colleagues in calling for a permanent extension of this program. In my State of Delaware, nearly 2,000 Delawareans last year received Perkins loans from 2013 to 2014. Those are 2,000 of my constituents who had the chance to go to college, invest in their education, improve their lives for the better, and that is in just 1 year of the program.

In the 50 years since Perkins was created, the program has awarded nearly $30 billion through 26 million loans across this entire country. Those are big, abstract numbers, but for my colleagues who remain undecided on whether to support the extension, I urge them to think about the Franks, the Taylors, their constituents, and folks from towns and cities, big and small, all across this country. They are not asking for a free education. The average Perkins loan is just $2,000. It is not even a rounding error in the scope of the total Federal budget that we fight over here week in and week out, but that is an amount that one student, one family can singlehandedly determine—for an aspiring teacher or a business owner or an inventor or someone who just wants to advance themselves through education—whether they can continue their steady forward progress.

This extension alone is not the Higher Education Act reauthorization many of us have been calling for; it is not the substantial education investment many of us know would be a huge boost to our country, its competitiveness, and our constituents' well-being; it is not a perfect solution to the Delawareans I talk to every day who wonder how they can afford college; it is an important start. So let's come together and act. Even the House of Representatives, of all places, has acted on a bipartisan basis to extend the Perkins Loan Program. We can and should do the same.

I thank my colleagues for their work on this critical issue, and I urge this Chamber to come together to approve an extension of the Federal Perkins Loan Program without delay.

Thank you. I yield the floor.

The PRESIDING OFFICER. The Senator from Pennsylvania.

Mr. CASEY. Mr. President, I rise to speak about the same subject that my colleague from Delaware just raised and so many others before him. It is bipartisan. This loan program, which we have had the luxury, I guess, all these years of relying upon, has allowed us to say that as a country we value higher education. We value that for no matter what family a person is from or what level of income. As I have often said, we believe not only in the context of early learning, when someone is at the beginning of their learning years, but much later when they are in the years of higher education, that they can learn more now and earn more later. That linkage, that direct nexus between learning and earning, is a substantial factor in whether someone can have a good job and a career and success in their life.

However, for a lot of folks, the cost of college, as so many have outlined today, becomes an impossible barrier over which they cannot climb, especially if they are low income. All they are asking for is a fair shot—a fair shot at learning, a fair shot at going to an institution of higher education.

We know this program has meant so much not only to folks across the country, but when we look State by State and examine the number of students, the number of families who are affected now, it is extraordinary, whether we are talking about the Presiding Officer's home State of Colorado or Senator COONS and his constituents in Delaware or Connecticut or Wisconsin or Ohio. Wherever we are, we can see the numbers.

In Pennsylvania, 40,000 students today are beneficiaries of the Perkins Loan Program. We are told as well that this isn't just a program that affects all different income levels; this is a program which is designed and has benefited those who most need it. We are told that one-quarter of recipients are from families with incomes of less than $30,000. The maximum loan amount per student is $5,500. If someone is going to a school where it costs $45,000 or $50,000, that may not seem like a lot, but for a lot of students who are at institutions that are not so high in cost, that is a big number—or a fraction of that number is a big number. If you are going to graduate school, you can get up to $8,000 from the Perkins Loan Program. It is a 10-year repayment period. As the Senator from Ohio pointed out, it is a revolving fund. So as one student is paying their Perkins loan back over 10 years, another student is benefiting from that revolving fund.

We have all had individuals in our States—I have talked a couple of times about Nikki Ezzolo. Nikki is a recent graduate of Edinboro University. She had a long and difficult pathway through her higher education years. She is a single mom. She was in school and then out of school. When she finally got through school and had the benefit of a Perkins loan, among other things, she said the following in talking about her own circumstances as a single mom:

> I am proud to be a college grad and my daughter is proud of me too. I am so grateful for getting a Perkins loan to help me. I know that I wouldn't be where I am right now—

Meaning with a job after graduating from Edinboro—

> without it, and that is a really scary thought.

So she is thinking about where she would have been without a Perkins loan. Where she would have been is highly likely out of school and therefore not working. And the job she got is with a major company in our State.

So that is Nikki.

I also mentioned on the floor a couple of weeks ago—and I will not repeat it, but I just want to remind folks of her name. Kayla McBride. She is a recent graduate of Temple University in Philadelphia. She is in one corner of the State in Philadelphia, the opposite corner of the State where Nikki went to school in Edinboro. She indicated she received a Perkins loan to help with tuition after her mother was laid off.

Then we have another example, someone I met during the break, right near my hometown. We were meeting with students all across the State about this issue. One of them was in Wilkes-Barre. His name is Anthony Fanucci, the student body President, and a senior at Wilkes University in Wilkes-Barre. Anthony's father works overtime to pay for his tuition, and Anthony works every weekend and two jobs over the summer. His Perkins loan helped him stay in school. I met Anthony and he spoke that day in public. Among the things he said was the following:

> My strengths got me to Wilkes University, but without financial funding, your strengths and your resume and what you've done before that mean nothing. I never ever seek pity for my financial situation because my financial situation is far from rare.

He is talking about so many students out there who face a fork in the road at some point. If they have Perkins, they can likely stay in school. If they don't have Perkins, many of them—far too many—will not be able to continue their higher education.

We know the program expired on September 30. Here is what it means for—here is the practical implications

for students. No new students can receive loans, and while the current recipients are ''grandfathered'' for 5 years, there is uncertainty because we have never been in this circumstance where the program has expired and we don't know exactly what will happen with regard to the implementation of any kind of new changes or new policy by the administration. It is important to note that some will not be benefiting from the grandfathering provision. A student would not be grandfathered if they do one of the following: if they change their major, if they alter their course of study, or if they transfer. I should also mention the cutoff for the grandfathering was June 30, 2015.

Let's consider one of those circumstances—if they change their major. We are told by a recent study in our State that 75 percent of students will change their major at some point in their years in college. Let's just say that it is 50 percent or 33 percent. Whatever the number is, that is a lot of students changing their major and thereby maybe taking themselves out of the protection of that grandfathering provision for Perkins loans now that we are in the period after it has expired.

Financial aid officials who have written to us talk about other circumstances. I won't read a full letter, but in one letter we got from a financial aid official they talked about ''significant changes in a family's financial circumstances'' and ''unexpected financial difficulties.'' That is the real world of real students and real families without Perkins or at least with the uncertainty with regard to Perkins. Neither situation in my judgment is acceptable. Not having a 1-year extension to a Perkins loan program makes no sense to me and to a lot of students. If we had an extension, we could debate if someone wanted to make changes or debate the elements of a program, but having it expire makes no sense. Even if the expiration doesn't definitively impact you, the uncertainty about that should not be part of a college student's experience. While they are studying, while they are getting through their coursework, especially as freshmen, they should have the certainty or at least the expectation that it will continue to help them.

In summary we should, No. 1, continue to work together in a bipartisan fashion to solve this problem. The good news is, despite the partisan rancor and divisions in Washington and in the Senate and the House, on this we have broad bipartisan support—something on the order of 28 co-sponsors, and at last count 6 are Republicans. So we have got folks in both parties working on this.

We all believe that we have an obligation to do everything we can to support higher education. No student should have to drop out of college because Congress has not done its job.

We have more work to do on this, and I would urge those who have concerns about it or want to have another point of view be debated, that I hope we could work together to get through this impasse and get the Perkins loan at least extended for 1 more year as was done in the House most recently by voice vote.

With that, Mr. President, I yield the floor.

The PRESIDING OFFICER. The Senator from Tennessee.

Mr. ALEXANDER. Mr. President, this discussion by very good Senators—and I congratulate the Senator from Pennsylvania and the other Senators who have spoken. The Senators from Pennsylvania and Wisconsin are both on the education committee and we have worked well together and we will continue to discuss this. This shows how difficult it is to do what most Americans have said they would like to see us do, which is to simplify, deregulate, and make it easier and simpler for students to go to college. That is what we are trying to do in the Senate.

Almost every witness who came before us said this: It is too complicated to fill out a form for the current form of student aid, so simplify it. The witnesses have said: Have one undergraduate student loan, have one loan for graduate students, and have one loan for parents. Right now undergraduate students might have three different loans with different interest rates and different terms.

The application process is so complicated that it turns away millions, we have been told, of students who are frustrated by that. The repayment program, which is very generous—not for the Perkins loan, which I will get to in a minute, but for all other direct loans—is so complicated that students don't take advantage of it.

We are toward the end of our work in the Senate education committee to take our giant student loan program, which loans more than $100 billion taxpayer dollars a year and has more than $1 trillion dollars of outstanding loans, and simplify it to make it easier and cheaper for students to go to college.

One way to do that is to replace the Perkins loan with a direct loan that has a lower interest rate and a more generous repayment plan. What we are proposing to do is to replace the Perkins loan with a direct loan that is available to every single student who is enrolled in an eligible accredited college. You show up, you enroll, you get the loan. That is available to you. The interest is 4.29 percent today. That is lower than your Perkins loan, and when you pay back the direct loan, you may pay it back like a mortgage over 10 years or you may pay it back over 20 or 25 years, not paying more than 10 or 15 percent of your disposable income. And if you haven't paid it back after those years, it is forgiven. That is what the taxpayers have said to the students. So that lower interest rate and generous repayment program are not a part of the Perkins loan program. What we, a bipartisan group of Senators, are saying is that we need to replace the Perkins loan with that better opportunity.

Let's be clear about who is affected by this. Perkins loans are about 1 percent of all student loans. So, about 99 percent of those students who have student loans are not affected by this discussion. Of those who have Perkins loans, you can keep your Perkins loan. The Department of Education notified all the institutions early in this calendar year and said the Perkins loan expires in the fall. If you grant a new Perkins loan this fall, it will be a 1-year loan. For everybody else who has already got a Perkins loan, you can keep receiving Perkins loans through the end of your program. So, in almost every case, you either got a 1-year loan if you got a new loan for the first time, or if you are already in a program, you keep it through to the end of your program. That is the situation.

It is important for students to know that the bipartisan effort here is to simplify the student loan program and give them a lower interest rate and a better repayment program. Why would you not want that instead of this? One might say we may want to have both. Sure, you would like to have both, but the Congressional Budget Office says it will cost $5 billion over 10 years to continue the Perkins loan program. The testimony we heard and our recommendation by this bipartisan group of Senators is we have a better use for that $5 billion.

We might have a higher amount of money that you could borrow. We know there are going to be more Pell grants granted if we simplify the application process and the repayment process. We would like to give students the opportunity to use their Pell grants year-round. Some way we have got to pay for that, and one way to pay for that is to simplify the system. If we take $5 billion to continue the Perkins loan program so we can give students a higher interest loan and a worse repayment program, we are also taking money away from the new Pell grants, from the possibility of a year-round Pell grant, and from the other reforms that we would like to make. Why should we be trying to change this now, when the Department has notified all the institutions that this is how things are going to be?

We are toward the end of our work in our committee. We work in a very good bipartisan way. We don't agree on everything; we don't expect to. But Senator MURRAY and I have the Elementary and Secondary Education Act. We expect to be able to do that with the Higher Education Act. The Senators will have a chance to offer amendments in the committee and on the floor. If the full Senate decides that it wants to keep the Perkins loan program and take $5 billion out of the funds available to give year-round Pell grants to students or the extra Pell grants that we would be able to grant by simplifying the application and instead continue a program with a higher

interest rate and a worse repayment program, then the full Senate can do that. I won't recommend it and I won't vote for it, but that is the purpose here.

It is important for everyone considering this to know that President Bush recommended that the program end. President Obama recommended that the program be changed and folded in, in effect, with the regular direct loan program.

The Federal Government hasn't contributed any new money to the Perkins loan program since 2004 because most people know that it is not as good a loan opportunity for almost all students. It is not as fair a use of the money as is the direct loan program.

I prefer private loan programs, but the Congress has decided it is a Federal loan program. To reemphasize, if you are enrolled in any accredited institution, and we have 6,000 of them, all you have to do is show up and you are eligible for the loan. We think you are better off. You will be less likely to over borrow and you will be more likely to go to college if it is a simpler program and if you have a single undergraduate loan, a single graduate loan, and a single loan for parents. That is the purpose behind my point of view on this.

This Senator would like for our committee to finish our work. Hopefully we can do that and give it to Senator MCCONNELL and let him put it on the floor early in the year, and the Senate can decide which loan programs it wants. If we want to continue the mumbo jumbo of student loan programs we have today, which discourage students from going to college and taking advantage of repayment programs and discourage the kinds of education that most of us want, then the Senate can do that, but I will be arguing against that.

That is why I asked the Senator from Arizona to object today to bringing immediately to the floor this continuation of a program that every institution in the country knew was supposed to end when it ended, and that one President has tried to end and another President has tried to change. Almost every witness that came before our committee said that students will be better off. Students are the ones we care about. As long as we are fair to taxpayers, students will be better off if we simplify the system and have a single undergraduate loan, a single graduate loan, and a single loan for parents.

In addition to that, there is a Federal grant system. If you are in Colorado or Tennessee or Connecticut or Pennsylvania and you want 2 years of college, for those who are eligible for the Pell grant, which you do not have to pay back, the 2 years of college is basically free. The average tuition for a 2-year community college is about $3,300 a year, and the average Pell grant is about $3,300 a year. So we are offering the students of this country—it is never easy to pay for college, but the taxpayers have been pretty generous. Basically, we are saying that everywhere in the country if you want 2 years of college and you are in the 40 percent of community college students that are lower income, your 2 years are basically free. If you need more money, you are entitled to a loan that you can pay back at an interest rate this year of 4.29 percent. That is a low interest rate for somebody with no credit rating and no collateral. You can't get that anywhere else, but you can get it from the Federal Government so you can go to college. We are saying in addition to that, you can pay it back over 20 years with your disposable income. If that isn't enough, if you are a teacher or fireman or someone who has not made as much to pay it back, it is forgiven by the taxpayers. We would like the Perkins loan students to have the lower interest rate and the more generous repayment program, and that is why I object to circumventing the committee's decisions.

Let us finish our work. Let us make a decision that we should be able to make as a whole Senate by early next year, and let the students who already have Perkins loans continue all the way through to the end of their program. Let the students who got it for the first time since July know that they will have that program for this 1 year. This is what every single university in the country was told about earlier this year and reminded of by the Department of Education in September.

Let's do this in an orderly way and let's put the students first. All of us are interested in helping students make it easier and simpler to attend college. I think our bipartisan proposal will replace the Perkins loan with a direct loan opportunity with a lower interest rate and a more generous repayment program. It is a better deal for students and avoids spending that $5 billion that I would like to use for the year-round Pell grant and for the additional Pell grants that are going to be created by a simpler student aid program.

I thank the Presiding Officer, and I yield the floor.

The PRESIDING OFFICER. The Senator from Connecticut.

Mr. BLUMENTHAL. Mr. President, I do respect the expertise and experience and dedication of my colleague and friend from Tennessee. I especially understand and am grateful for his leadership as the chairman of the Health, Education, Labor and Pensions Committee, which has jurisdiction over this legislation. I understand that he is moving toward reform and overhaul of the current system of financial aid and loans that will make it better for students. That is the goal, that it will be ready perhaps sometime early next year.

As we know from our experience in this body, timelines frequently shift and give way. So early next year may turn into later next year or the spring of next year or at some point in time. In the meantime, futures are in the balance—the futures of students in Connecticut and around the country who are trying to plan in their senior year. Their faces and voices are with me and with all of us every day. Their futures are the future of this country.

The House has extended the Perkins Loan Program for 1 year. Why won't the Senate do it? My colleague from Tennessee urges that we simplify the program. Well, let's simplify decisions that are being made right now at the kitchen tables and the living rooms of families across the country and make available this option even as we simplify and reform the program because the failure to do so vastly complicates and confuses the lives of students who are making real-life decisions while we debate. We are, in fact, debating right now a cyber security information sharing act which pertains to the cloud and computing that takes place in the cloud. We are talking here in the clouds compared to real-life decisions being made by students and their families every day. I am hearing from them. I am hearing from financial aid administrators, for example at Quinnipiac University in Hamden, CT, who tell me that there is a level of anxiety and angst they have not seen in recent years because of this body's inaction, its failure to continue a program that has worked and worked well for countless students. In fact, in the 2014–2015 school year, institutions in Connecticut disbursed over $20 million through the Perkins Loan Program, using that funding to provide targeted financial aid to support their very neediest students. Low-income students who face a gap in funding and who have to make hard decisions about real dollars and cents need this program not early next year but right now.

The Senate's failure to act, as the House has done, to extend it for 1 year, abrogates its responsibility. In previous years, Quinnipiac, for example, would have been able to offer these students Perkins loans to close the gaps between what financial aid they are receiving and what they need to continue their education. This year, they are telling students: Sorry, no help available.

These students are the future of our country. They are the ones who are going to be doing the computer science that is necessary for our cyber security. They are the intellectual infrastructure of this country. Our failure to invest in them—and this expiration is only one reflection of that failure to invest—is a failure for the entire country.

I received a note from Nicole Deck—a sophomore at the University of New Haven—telling me how she benefitted from the Perkins program. She is pursuing a double major in marine biology and environmental science. She wrote to me saying: ''I appreciate every day that I spend at the University of New

Haven thanks to the aid of the Federal Perkins loans.''

She said: ''Receiving money from the Federal Perkins Loan has allowed me to achieve many of my goals and has opened many doors of opportunity.''

The doors of opportunity for Nicole in marine biology and environmental science on the shores of Long Island Sound, where she can put that science to work to help to save Long Island Sound and to help us nationally to preserve our environment, are not only doors of opportunity for her, they are doors of opportunity for our whole country. The failure to extend the Perkins loan program closes those doors.

I met recently with seniors at the New Britain High School. At New Britain High School, these seniors are thinking about where they will be going to school. They are making life-changing and transformative decisions about their futures based on their financial alternatives. When I asked them ''How many of you have, in effect, abandoned the school of your first choice because you couldn't afford it and Federal aid was not available and no scholarships were accessible?'' about half of them raised their hands.

I thought to myself, well, things often work out for the better but sometimes not. Sometimes futures are constrained and warped and distorted because a young person with great potential is unable to develop it because of an avenue of education blocked by financial unaffordability.

My colleagues have stated very powerfully and eloquently and it has been a bipartisan debate about what the Perkins Loan Program means to so many students.

I will close by saying that this program involves an example of real institutional skin in the game. It requires institutional capital contributions as a requirement for a school's participation. It fills the gap of affordability that affects our very neediest and often most deserving students.

Our constituents will rightly ask us: Did you reject the student loan program?

No, we did not reject it.

Did you renew it?

No. We simply allowed it to die.

This program has gone into the cloud. We have allowed this to expire when we could extend it for 1 year without really damaging the reform effort underway.

I want to repeat that I respect the HELP Committee chairman's intention and goal to reform all student loan programs, but in the meantime, futures of American students are affected unfairly and unwisely by the inaction by this body.

I yield the floor.

The PRESIDING OFFICER. The Senator from Tennessee.

Mr. ALEXANDER. I thank the Senator from Connecticut for his eloquent remarks. Let me offer this different perspective. You don't need a Perkins loan to go to a 2-year college. The average tuition at a community college—and they are a terrific opportunity in my State and most States—is about $3,300. About 40 percent of the students who attend them qualify for a grant of about, on average, $3,300. So those 2 years are free for most students who need the money. Those students are also entitled to a direct loan if they enroll at the community college. Usually it is $4,000, $5,000, to $6,000. They just walk up and they are entitled to it if they think they need it.

You probably don't need a Perkins loan to go to most of the State universities. At the University of Tennessee, the tuition and fees is about $12,000. Many of the best colleges and universities are State institutions.

You are entitled to your Pell grant. You are entitled to your direct loan. Then many States and universities have their own programs. For example, in Tennessee there is the HOPE Scholarship, and almost all of the students at the University of Tennessee Knoxville have one.

Where the Perkins loan has been useful—and I will grant that—has been at the expensive private colleges. If it is $50,000 a year to go to a private college, you can get your Pell Grant, you can get two direct loans, and then you can get a Perkins loan. Then you can end up being in the newspaper for having borrowed so much that people write articles in the Wall Street Journal about how we have created a circumstance where students are overborrowing and cannot pay back their student loans.

So I think the question really is, Should taxpayers spend $5 billion more over the next 10 years to make it possible for a the student to go to a $50,000-a-year tuition school or should taxpayers spend that money to create a year-round Pell Grant and hundreds of thousands of additional Pell Grants for low-income students who want another 2 years or 4 years of education? I think that is the question.

Government is about setting priorities. If we had an unlimited amount of money, we could do everything. Except, we do have a problem with overborrowing and complexity. When you add a third loan on top of two other loans so that can you go to a $50,000-a-year tuition college, that is a choice an American has to make. I am proud of the fact that we have those choices. But we have lots of 18-, 19-, 20-year-olds, and many graduate students, too, who 5 or 10 years later will find they cannot pay it back.

I think we are better off with a single undergraduate loan, a single graduate loan, and a single parent loan that is available to every single student. I think we are better off using whatever savings we have to expand the number of Pell Grants and to offer a year-round Pell Grant.

As I said before, every single institution—all 6,000 of our institutions were told by the Department of Education earlier in 2015: If you grant a Perkins loan this fall to someone who never received one before, it will be for 1 year because the program is ending.

Also, they were told: If someone already has a Perkins loan, you will be able to keep it all the way through the end of their program.

So this is an honest difference of opinion. There are a lot of university presidents—I know a bunch of them. They like the program because it gives them one more tool to use. The question is not just whether they like the program; the question is, What is best for the students? I think taking the available amount of money we have and expanding it for simplifying the student aid system and making the year-round Pell and the other programs available to students who need it the most—I think that is what we should be doing.

We will finish our work in the Senate education committee hopefully within a few weeks. We will have it ready to come to the floor. We can debate it, and the Senator from Connecticut and I can continue our discussion.

I yield the floor.

The PRESIDING OFFICER. The Senator from Arizona.

AMENDMENT NO. 2582

Mr. FLAKE. Mr. President, I rise to speak in support of the Flake amendment No. 2582 that is currently pending before the body. This amendment is very simple. It simply adds a 6-year sunset to the bill. This amendment also keeps in place the liability protections established by the Cyber Security and Information Sharing Act for information that is shared pursuant to the requirements of the bill. Furthermore, the amendment ensures that the requirements on how the information is shared under the act is to be handled remain in effect after the sunset date.

That is all this amendment does. It simply sunsets the bill in 6 years, and it does so in a reasonable and responsible way. I believe in the sunset provision. It is good for us to consider our past decisions 6 years from now, to determine whether what we enacted is operating well, and to debate the overall success of the legislation that we passed 6 years prior. We ought to do that, frankly, on a lot of other legislation we pass.

I do believe the bill we are currently considering, as it is written, strikes the right balance. It puts in place the proper privacy protections, and I plan to support the legislation. However, it is important to make sure that we are forced to go back and evaluate it in the years to come to make sure we actually got it right. Given the nature of the bill being debated before us, it is all the more important to do so in this instance.

I would also note that this 6-year sunset is similar to sunset provisions that were included in both House-passed cyber security bills. So if it is in the House, we ought to have it in the Senate as well.

Both the Protecting Cyber Networks Act, which passed the House by a vote

of 307 to 116, and the National Cybersecurity Protection Advancement Act, which passed the House by a vote of 355 to 63, include a 7-year sunset.

I ask my colleagues to support this amendment. I think it does strengthen the bill. It ensures that we evaluate, as we should, any legislation that we pass to ensure that it is having its intended effect.

I yield back the remainder of my time.

I suggest the absence of a quorum.

The PRESIDING OFFICER (Mr. LEE). The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

The PRESIDING OFFICER. The Senator from Louisiana.

Mr. VITTER. I ask unanimous consent that the order for the quorum call be rescinded.

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

UNANIMOUS CONSENT REQUEST—S. 697

Mr. VITTER. Mr. President, I rise in strong support of the Frank R. Lautenberg Chemical Safety for the 21st Century Act. Over 2 years ago, I sat down with now the late Senator Frank Lautenberg of New Jersey in an attempt to find compromise and to work together on updating the drastically outdated Toxic Substances Control Act. Updating this law was a long-time goal and passion of Frank's. It was a real goal of mine, although we came at it from very different directions, at least initially. I am saddened Frank isn't here with us to see it finally being brought up for consideration on the floor of the Senate. We worked closely together and forged a significant, productive, positive bipartisan compromise—the sort of work we don't see often enough in the Senate or the Congress itself, but we got it done here, and it is a strong, positive compromise in substance as well.

After Frank's passing, Senator TOM UDALL stepped in to help preserve Frank's legacy and continued working with me to move this reform forward. We have done that consistently over months and months, working on issue after issue, detail after detail, to produce a strong result. I am very proud of the substance of this result because it achieves two very important goals: On the one hand, we certainly protect health and safety and give the EPA the proper authorities to do that with regard to chemicals in commerce. On the other hand, we make sure we don't overburden industry and put them at a disadvantage in terms of remaining America's world leaders in innovation and chemistry. We are world leaders now. We innovate, we produce new chemicals and new uses and new products on a spectacular basis, and we certainly don't want to threaten that. Our Frank R. Lautenberg Chemical Safety for the 21st Century Act doesn't threaten it. It enhances it, it protects health and safety, and that is why I am so proud of this bipartisan work.

We have done that work so completely we are now in a position to pass this bill through the Senate in very short order. In fact, we only need 2 hours of floor time, and we need no amendment votes related to the bill in any way. That is virtually unheard of in the Senate, but it goes to the work that so many folks have done on both sides of the aisle. So with 2 hours of floor time, no amendment votes, we can pass this bill and move it on to the House. We have been in contact with the House for months, so we are very hopeful we can follow up our action with House action and a final result in relatively short order.

Mr. President, that is why we are coming to the floor today, to ask unanimous consent to establish that process in the near future—a very simple, very short process so we can get this done and achieve this result. Again, no amendment votes are necessary—whether they are germane, related or unrelated, no amendment votes are necessary—and then pass it on to the House. I certainly hope we can have that agreement to move forward in a productive fashion.

With that, let me yield to my Democratic colleague Senator UDALL, who has been such a great partner in this effort following Frank Lautenberg's unfortunate passing.

The PRESIDING OFFICER. The Senator from New Mexico.

Mr. UDALL. Mr. President, I thank my colleague Senator VITTER. It has been a real pleasure working with him on the Toxic Substances Control Act. I think we have brought this a long way.

First, let me speak on the pending cyber security legislation, and then I will be seeking unanimous consent to process another bill.

Protecting our national security and economic interests from cyber attack is a very important priority. I commend Senator BURR and Senator FEINSTEIN for their hard work on their legislation. I know they have also gone through a lot to get floor time on their bill and are working to process amendments. It is clear they have made a serious effort. I respect the chairman, vice chairman, and their staffs for their work.

My understanding is this will pass with a large bipartisan majority in the Senate. As Chairman BURR stated yesterday, the House has already acted on cyber security legislation. He is eager to start reconciling differences and get a bill to the President's desk. That is what good legislators do.

As the chairman knows, I have also been working for a number of years on a complicated legislative project, working with Senator VITTER, Senator INHOFE, and many other Senators of both parties. We are very close to the reform of the totally outdated Toxic Substances Control Act. We all know TSCA is broken. It fails to protect families and it fails to provide confidence in consumer products. We have a chance today to change that and to show that Congress can actually get things done.

I am pleased Chairman BURR is a cosponsor of our legislation, along with over half of the Senate. After years of work, we are now also in a position to seek unanimous passage of TSCA reform so we can go to conference with the House of Representatives. It has been a long road with lots of productive debate and discussion and cooperation and compromise. This is a balanced bill, one that Republicans, Democrats, industry, and public health groups can all support moving forward.

Not everyone loves our Senate product, but its staunchest opponents are now ready to allow for Senate passage. We can then reconcile our bill with the House, just as Senator BURR seeks to do on cyber security legislation. We have cleared this legislation on the Democratic side of the aisle with a short time agreement. My understanding is that there is nearly unanimous consent—unanimous signoff—on the Republican side as well.

With that, I join with Senators VITTER and INHOFE in asking for unanimous consent. I ask unanimous consent that at a time to be determined by the majority leader, in consultation with the Democratic leader, the Senate proceed to the consideration of Calendar No. 121, S. 697; further, that the only amendment in order be a substitute amendment to be offered by Senator INHOFE; that there be up to 2 hours of debate equally divided between the leaders or their designees; and that following the use or yielding back of that time the Senate vote on adoption of the amendment, the bill be read a third time, and the Senate vote on passage of the bill, as amended, if amended, with no intervening action or debate.

The PRESIDING OFFICER (Mr. VITTER). Is there objection?

Mr. BURR. Reserving the right to object.

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Mr. President, let me say to the authors, I have deep respect for both of you, and you have done an incredible job with this bill. It is one of the reasons I am a cosponsor, because it is good legislation.

It is no surprise to the Senate that I have had a deep desire to add the Land and Water Conservation Fund reauthorization, which has expired, as an amendment to this bill. I seek no time. I only seek the vehicle for an up-or-down vote and a ride—a ride that I can't seem to get by itself. As a matter of fact, I think the authors of this bill know that I have said if somebody can offer me a stand-alone opportunity to debate and vote on the Land and Water Conservation Fund, we can unanimous consent TSCA. We can't achieve that. I certainly don't want to take anything away from what I think is a great bill, and I wouldn't even require time, I would only require a vote.

So I would ask the authors to modify their unanimous consent request to include a vote on the Burr-Ayotte-Bennet amendment in relation to the Land and Water Conservation Fund.

The PRESIDING OFFICER. Will the Senator so modify his request?

Mr. BURR. I ask unanimous consent that the consent be modified to include a vote on the Burr-Ayotte-Bennet amendment in relation to the Land and Water Conservation Fund.

The PRESIDING OFFICER. Will the Senator so modify his request?

Is there objection to the modification?

The Senator from Utah.

Mr. LEE. Mr. President, reserving the right to object, we have an opportunity to update and reform the Land and Water Conservation Fund, and to do so in a way that would ensure it works more efficiently and helps solve the problems facing our Federal Government and States. To do so, we need to pursue a few goals.

First, more money from the LWCF should be sent to the States to implement the worthwhile projects. When the LWCF was conceived, 60 percent of its funding was required to go to the States. That statutory requirement was removed years ago, and now just 12 percent of LWCF money is given to the States, with minimal Federal strings attached.

Next, the LWCF should be used to solve, not to exacerbate, the current Federal lands maintenance backlog. The Federal Government has undertaken an impossible task in trying to manage more than 600 million acres of variant terrain dispersed across thousands of miles. Evidence of the Federal Government's failure to manage its holdings is found in the $13 billion through $20 billion maintenance backlog, a number that has grown nearly every single year since President Obama has been in office.

Since LWCF was created some 50 years ago, Congress has appropriated nearly $17 billion to the fund, and 62 percent of this money has been spent on land acquisition, resulting in 5 million acres being added to the Federal estate.

We should work together to improve the LWCF. Let's work together to make sure that North Carolina, New Hampshire, New Mexico, and every other State in this country gets more money. Let's work together to make sure that the Federal Government only acquires such land as it can adequately manage.

On that basis, I object.

The PRESIDING OFFICER. Objection is heard.

Is there objection to the original request?

Mr. BURR. I object.

The PRESIDING OFFICER. Objection is heard.

The Senator from New Mexico is recognized.

Mr. UDALL. Mr. President, again, I respect Senator BURR, but I am very disappointed in that objection. I take a back seat to no one in supporting the Land and Water Conservation Fund. It is extremely popular in New Mexico and critical to enabling our outdoors economy. Senator BURR has been a strong leader on the LWCF. He has brought much needed attention and passion to the issue of reauthorization, and I want to work with him on that. But the current strategy of holding TSCA hostage for LWCF is not the proper one. This is the sort of thing that gives the Senate a bad reputation for dysfunction, and I do not see how it will lead to any progress on LWCF. I have not objected to Senator BURR's efforts to pass reauthorization in the Senate. In fact, I have appraised his efforts. I share his frustration that a small minority of Republicans have blocked his efforts. But now, instead of one bill being blocked, we have two. Without this objection, TSCA would pass today almost unanimously after years of hard work.

So instead of holding TSCA hostage, why not consider LWCF on Senator BURR's legislation?

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

The PRESIDING OFFICER (Mr. LEE). Without objection, it is so ordered.

SUPERSTORM SANDY RELIEF AND DISASTER LOAN PROGRAM IMPROVEMENT ACT OF 2015

Mr. VITTER. Mr. President, in the small business committee, we have been working on significant legislation that goes to disaster recovery, the Superstorm Sandy Relief and Disaster Loan Program Improvement Act. We are ready to move that legislation and pass it through the entire Senate.

Since Hurricane Katrina devastated my State of Louisiana in 2005, I have fought to support disaster victims and improve the efficiency and effectiveness of our Nation's disaster relief and recovery efforts. I have continued this vital focus on disaster mitigation and recovery as Chairman of the Committee on Small Business and Entrepreneurship. I stand by my principle that when people are there for you, you will be there for them. Following my brief remarks, I will ask unanimous consent that the Senate pass H.R. 208, which has passed the House unanimously, with the Vitter amendment.

With Superstorm Sandy, similar to after Katrina, we continued to see—and both the GAO and IG confirmed—significant shortcomings with the SBA's disaster loan programs, particularly application processing times and inaccurate information, which discouraged victims from applying for assistance. H.R. 208 reopens the SBA disaster loan program to those victims for one year, and also includes vital reforms and oversight to the SBA's disaster loan program. This bill does not cost anything as the funds have already been appropriated but sit unused.

The RISE After Disaster Act, which is included in my amendment, passed out of the Small Business Committee with unanimous support, and will provide long-term recovery loans to small businesses through community banks after SBA disaster assistance is no longer available; direct Federal agencies to utilize local contractors for response and recovery efforts, rather than government contractors from Washington, DC, and other areas; address contractor malfeasance, such as the Chinese drywall crisis, by allowing homeowners and businesses to use their SBA disaster loans to remediate their property; provide incentives for innovative firms doing research and development to stay in the disaster-affected area, rather than move elsewhere; and require the SBA to take steps to establish a web portal for disaster assistance, whereby applicants can track the status of applications and approvals, as well as submit required supporting documentation electronically.

Hurricanes Katrina and Rita in 2005, Sandy in 2012, and Joaquin just this month—along with far too many other natural disasters—have all illustrated the devastating effects of hurricanes and flooding on our communities. As Chairman of the Senate Small Business and Entrepreneurship Committee, I am committed to serving small businesses across the country and ensuring that they are afforded the resources and assistance in order to protect themselves from and recover after disasters.

This means rigorous oversight of the SBA's disaster loan programs and extensive examination of economic recovery efforts, agency coordination, and the efficiency of disaster assistance delivery. Small businesses are vital to every community's economy and serve as the major source of jobs—one great incentive to have folks return after a major disaster—and is why helping them to more quickly recover is one of the most effective and beneficial tactics we can and should take.

Mr. President, I ask unanimous consent that the Committee on Small Business and Entrepreneurship be discharged from further consideration of H.R. 208 and the Senate proceed to its immediate consideration.

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

The clerk will report the bill by title.

The legislative clerk read as follows:

A bill (H.R. 208) to improve the disaster assistance programs of the Small Business Administration.

There being no objection, the Senate proceeded to consider the bill.

Mr. VITTER. Mr. President, I ask unanimous consent that the Vitter amendment, which is at the desk, be agreed to, the bill, as amended, be read