and our military. With this agreement the Republican leader just mentioned, we have done just that. Democrats and Republicans have come to a responsible agreement that puts the needs of our Nation above the Republicans' partisan agenda. While this agreement is not perfect, it does address both investment in domestic priorities that benefit the middle class and defense spending. It helps us avoid a major threat to jobs and the general economy. The time to do away with the devastating sequester cuts that are harming our middle class and military is not in the future. It is right now. Democrats hope to end sequestration for the good of our great country.

Our work is not done. I hope that we can continue to work together—Democrats and Republicans—to pass this legislation and place the priorities of the American people ahead of partisan politics.

CYBER SECURITY LEGISLATION AND CLIMATE CHANGE

Mr. REID. Mr. President, it was 3 years ago this month that then-Secretary of Defense Leon Panetta warned the United States of a potential ''cyber Pearl Harbor.'' A cyber Pearl Harbor would be crippling, and it would be a cyber attack on our Nation's banks, power grid, government, and communications network.

If it sounds scary, that is because it is scary. Cyber terrorists could potentially bring the United States to its knees. This potentiality is upon us. A catastrophic cyber attack is not farfetched. Ted Koppel, the renowned journalist, has written another book, and the author reveals that our Nation's power grid is extremely vulnerable to cyber terrorism. Imagine the toll of these attacks: massive power blackouts, no telephone, no Internet capability—that is on your cell phones or whatever phones exist—overwhelmed first responders and an infrastructure system reduced to chaos.

How vulnerable is our Nation to a cyber attack of this magnitude?

Former Secretary of Homeland Security Janet Napolitano, in the book that was written, as I indicated, by Ted Koppel, stated that the likelihood of an attack on our Nation's power grid is 80 to 90 percent—80 percent to 90 percent.

Craig Fugate, the Administrator of the Federal Emergency Management Agency, has had to think about a potential cyber attack. It is his job. Listen to his assessment:

> We're not a country that can go without power for a long period of time without loss of life. Our systems, from water treatment to hospitals to traffic control to all these things that we expect every day, our ability to operate without electricity is minimal.

A number of years ago we had, at the direction of Senator MIKULSKI—a longtime member of the Intelligence Committee—a meeting where such an attack was discussed and the implications of it. That was years ago. It was frightening then, and it is even more frightening now. But as Mr. Fugate indicated, that is the scale of threat the United States faces with cyber terrorism.

We as a country must do more to protect ourselves against this cyber terrorism. It can be done if Republicans will work with us. Democrats tried to pass comprehensive cyber security legislation years ago. What happened? It was filibustered by the Republicans. They wouldn't even let us on this legislation. They wouldn't even allow us to debate the bill. Whatever their reasoning, I am glad the Republicans have finally changed course in this decision and allowed this simple bill to move forward. We support this legislative effort, but we recognize that it is far, far too weak.

Cyber terrorism and cyber attacks are part of today's world. But Republicans are denying the seriousness of this, as they are denying something clear to everyone in the world except my Republican Senate and House Members. We have climate change taking place that is really hurting everybody, with rare, rare exception. Cyber terrorism and cyber attacks are part of today's world, just like climate change. To not move forward with more comprehensive cyber security legislation and to ignore what is happening in our world dealing with climate change will in the years to come be considered legislative malpractice. I am sorry to say that legislative malpractice is not on our shoulders. We wanted for years to do something with climate change. We can't. It is not even something that the Republicans will allow us to discuss. We wanted for years to do something with cyber security. They refused to do so. We have a bill before us that is better than nothing, and we support it. But it is far, far too weak.

Mr. President, I see the assistant Democratic leader on the floor. Would the Chair announce before he talks to us what we are going to do here today.

RESERVATION OF LEADER TIME

The PRESIDING OFFICER. Under the previous order, the leadership time is reserved.

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 senior assistant 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 ten years.

Feinstein (for Franken) further 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.

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.

The PRESIDING OFFICER. Under the previous order, the time until 11 a.m. will be equally divided between the two leaders or their designees.

The assistant Democratic leader.

Mr. DURBIN. Mr. President, the debate which we will engage in today on the floor of the Senate is really one that parallels the historic debates that have occurred in the course of our Nation's history. When a great democracy sets out to defend its citizens and to engage in security, it really is with a challenge: Can we keep our Nation safe and still protect our rights and liberties? That question has been raised, and that challenge has been raised time and again.

It was President Abraham Lincoln during the Civil War who suspended the right of habeas corpus. It was challenged by some as an overextension by the executive branch, but President Lincoln thought it was necessary to resolve the Civil War in favor of the Union. In World War I, the passage of the Alien and Sedition Acts raised questions about the loyalty of Americans who question many of the great issues that were being raised during that war. We certainly all remember what happened during World War II when, even under President Franklin Roosevelt, thousands of Japanese Americans were interned because of our concerns about safety and security in the United States. It continued in the Cold War with the McCarthy hearings and accusations that certain members of the State Department and other officials were, in fact, Communist sympathizers. That history goes on and on.

So whenever we engage in a question of the security and safety for our Nation, we are always going to be faced

with that challenge. Are we going too far? Are we giving too much authority to the government? Are we sacrificing our individual rights and liberty and privacy far more than we should to keep this Nation safe? That, in fact, is the debate we have today on the most sophisticated new form of warfare—cyber war.

Cyber security is an enormous concern not just for private companies but for every American. Data breaches happen almost every day. We read not that long ago that 21 million current and former Federal employees had their records breached and stolen from the Office of Personnel Management. Just this month more than 700,000 T-Mobile users in my home State may have had their information compromised by hackers. It seems there isn't a month that goes by where we don't hear of another security breach. That is why we need to take steps to improve data security and share cyber threat information.

Chairman BURR and Ranking Member FEINSTEIN worked long and hard to put together a bill to encourage private and governmental entities to share potential threat information. This bill has evolved over 5 years. No one has worked harder during that period of time than my colleague, Senator FEINSTEIN of California. Senator BURR is now joining her in this effort.

Many are skeptical about the bill before us. Some have raised those concerns on the floor. But we look at the major companies that are opposing this bill as currently written—Apple, IBM, Microsoft, Google, Facebook, and Amazon—just a few of the major companies that have said they can't support the bill that is on the floor today. They note that the bill does not require companies or the Federal Government to protect private information, including personal emails, email addresses, and more. In fact, this bill preempts all laws that would prevent a company or agency from sharing personal information.

I am encouraged that the managers of this bill have moved in the direction of addressing this concern. They have limited the authorization to share cyber threat information to ''cyber security purposes''—a valuable step toward making sure the bill is not used as surveillance. They have included a provision requiring government procedures to notify Americans if their information is shared mistakenly by the government. They have clarified that the authorization to employ defensive measures—or defensive ''hacking''—does not allow an entity to gain unauthorized access to another's computer network.

There will be some amendments before us today that I will support which I think strengthen the privacy protections that should be included in this bill.

I am a cosponsor of the Franken amendment to improve the definitions of ''cyber security threat'' and other cyber threat indicators. Narrowing this definition from information that ''may'' be a threat to information that is ''reasonably likely'' to pose a threat would reduce the amount of potentially personal information shared under the bill.

I also urge my colleagues to support the Wyden amendment to strengthen the requirement that private companies remove sensitive personal information before sharing cyber threat indicators. Again, this amendment would limit the amount of potentially personal information shared under the bill.

I support the Coons amendment to give the Department of Homeland Security time to remove or scrub personal information from the information it shares with other Federal agencies. There is simply no need for personal information unrelated to a threat to be shared with law enforcement agencies such as the Department of Justice and NSA.

These amendments would strengthen privacy protections in the bill much more than the original managers' package. I look forward to working with Senators BURR and FEINSTEIN and others to ensure that the final bill addresses our cyber security concerns while still protecting privacy—something I know we all want to do.

Mr. President, I yield the floor.

Mrs. FEINSTEIN. 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 the roll.

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

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

Mrs. FEINSTEIN. Mr. President, I ask unanimous consent that the time be charged equally on both sides.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

Mrs. FEINSTEIN. I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The senior assistant 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, shortly we will once again begin the process on the cyber security bill. We will start votes hopefully right at 11 o'clock. We will try to work through five amendments this morning and return this afternoon with a short period of debate, and once again, at 4 o'clock, we will take up five additional votes—or possibly four—and be at the point where we could conclude this legislation.

Let me say to my colleagues that the Senate has tried for several years now to bring cyber security legislation to the Senate floor and find the will to pass it. With the work of the vice chairman, I think we have been able to succeed in that. We enjoyed a 14-to-1 vote out of the committee, showing tremendous bipartisan support. Thousands of businesses and almost 100 organizations around the country are supportive of the bill. But, more importantly, in the last several days the bill has gained the support of the Wall Street Journal and the Washington Post—not necessarily publications that chime in on the need for certain pieces of legislation from the Senate floor, but in this particular case, two publications understand the importance of cyber security legislation getting signed into law.

This is the first step, and conferencing with the House will come shortly after. I am proud to say that we already have legislation the White House says they support. So I think we are in the final stretches of actually getting legislation into law that would voluntarily allow companies to partner with the Federal Government when their systems have been breached, when personal data is at risk.

I still say today to those folks both in this institution and outside of this institution who are concerned with privacy that I think the vice chairman and I have bent over backward to accommodate concerns. Some concerns still exist. We don't believe they are necessarily accurate and that only by utilizing this system will, in fact, we understand whether we have been deficient anywhere.

There are also several companies that are not supportive of this bill, as is their right. I will say this: From the beginning, we committed to make this bill voluntary, meaning that any company in America, if its systems are breached, could choose voluntarily to create the partnership with the Federal Government. Nobody is mandated to do it. So I speak specifically to those companies right now: You might not like the legislation, but for goodness' sakes, do not deprive every other business in America from having the opportunity to have this partnership. Do not deprive the other companies in this country from trying to minimize the amount of personal data that is lost because there has been a cyber attack. Do not try to stop this legislation and put us in a situation where we ignore the fact that cyber attacks are going to happen with greater frequency from more individuals and that the sooner we learn how to defend our systems, the better off personal data will be in the United States of America.

This is a huge deal. The vice chairman and I from day one have said to our Members that we will entertain any good ideas that we think strengthen the bill. On both sides of the aisle, we have said to Members that if this breaks the agreement that we have for the support we need, because they don't believe the policy is right, then

we will lock arms and we will vote against amendments.

We have about eight amendments today. On a majority of those, we will do that. I am proud to tell my colleagues that during the overnight and this morning—we will announce today that we have taken care of the Flake amendment with a modification. We are changing the sunset on the legislation to 10 years, and we will accept the Flake amendment on a voice vote later this morning. We continue even over these last hours to try to modify legislation that can be agreed to on both sides of the aisle but, more importantly, without changing the delicate balance we have tried to legislate into this legislation.

I am sure Members will come down over the next 35 minutes, but at this time I will yield the floor so the vice chairman can seek time.

The PRESIDING OFFICER. The Senator from California.

Mrs. FEINSTEIN. Thank you, Mr. President.

I wish to begin by thanking the chairman for his work on the bill.

For me, this has been a 6-year effort. It hasn't been easy. It hasn't been easy because we have tried to strike a balance and make the bill understandable so that there would be a cooperative effort to share between companies and the government.

Last Thursday the Senate showed its support for moving forward with two strong votes. We had a vote of 83 to 14 to invoke cloture on the substitute amendment, showing that there is, in fact, deep bipartisan support for moving significant legislation to the President's desk.

To that end, I ask unanimous consent that editorials from the two major U.S. newspapers be printed in the RECORD.

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

[From the Washington Post, Oct. 22, 2015]

THE SENATE SHOULD TAKE A CRUCIAL FIRST STEP ON CYBERSECURITY

(By Editorial Board)

After years of failure to find a consensus on cybersecurity, the Senate is expected to vote early next week on a bill that would enable the government and the private sector to share information about malicious threats and respond to them more quickly. The legislation is not going to completely end the tidal wave of cyberattacks against the government and corporations, but passing it is better than doing nothing—and that is where Congress has left the matter in recent years.

The legislation, approved by the Senate Select Committee on Intelligence on a bipartisan 14–to-1 vote in March, is intended to iron out legal and procedural hurdles to sharing information on cyberthreats between companies and the government. Private-sector networks have been extremely vulnerable, while the government possesses sophisticated tools that might be valuable in defending those networks. If threats are shared in real time, they could be blunted. The legislation is not a magic wand. Hackers innovate destructive and intrusive attacks even faster than they can be detected. The information sharing would be voluntary. But the bill is at least a first step for Congress after several years of inconclusive debate over how to respond to attacks that have infiltrated networks ranging from those of Home Depot to the Joint Chiefs of Staff.

The biggest complaint about the bill is from privacy advocates, including Sen. Ron Wyden (D–Ore.), who cast the sole dissenting vote on the intelligence committee. His concerns have been amplified recently by several tech giants. Apple told The Post this week that it opposes the legislation because of privacy concerns. In a statement, the company said, ''The trust of our customers means everything to us and we don't believe security should come at the expense of their privacy.'' Some other large technology firms are also opposing the bill through a trade association. Separately, alarmist claims have been made by privacy advocates who describe it as a ''surveillance'' bill.

The notion that there is a binary choice between privacy and security is false. We need both privacy protection and cybersecurity, and the Senate legislation is one step toward breaking the logjam on security. Sponsors have added privacy protections that would scrub out personal information before it is shared. They have made the legislation voluntary, so if companies are really concerned, they can stay away. Abroad coalition of business groups, including the U.S. Chamber of Commerce, has backed the legislation, saying that cybertheft and disruption are ''advancing in scope and complexity.''

The status quo is intolerable: Adversaries of the United States are invading computer networks and hauling away sensitive information and intellectual property by the gigabyte. A much stronger response is called for in all directions, both to defend U.S. networks and to punish those, such as China, doing the stealing and spying. This legislation is a needed defensive step from a Congress that has so far not acted on a vital national concern.

[From the Wall Street Journal, Oct. 26, 2015]

A CYBER DEFENSE BILL, AT LAST

DATA SHARING CAN IMPROVE SECURITY AND CONSUMER PRIVACY

By now everyone knows the threat from cyber attacks on American individuals and business, and Congress finally seems poised to do something about it. As early as Tuesday the Senate may vote on a bill that would let businesses and the government cooperate to shore up U.S. cyber defenses.

This should have been done long ago, but Democrats blocked a bipartisan bill while they controlled the Senate and President Obama insisted on imposing costly new cyber-security mandates on business. The GOP Senate takeover in 2014 has broken the logjam, helped by high-profile attacks against the likes of Sony, Home Depot, Ashley Madison and the federal Office of Personnel Management.

Special thanks to WikiLeaks, the anti-American operation that last week announced that its latest public offering would be information hacked from the private email account of CIA chief John Brennan. We assume Mr. Brennan's government email is better protected, but then this is the same government that let Hillary Clinton send top-secret communications on her private email server.

Democrats have decided it's now bad politics to keep resisting a compromise, and last week the Cybersecurity Information Sharing Act co-sponsored by North Carolina Republican Richard Burr and California Democrat Dianne Feinstein passed the filibuster hurdle. A similar bill passed the House in April 307–106.

The idea behind the legislation is simple: Let private businesses share information with each other, and with the government, to better fight an escalating and constantly evolving cyber threat. This shared data might be the footprint of hackers that the government has seen but private companies haven't. Or it might include more advanced technology that private companies have developed as a defense.

Since hackers can strike fast, real-time cooperation is essential. A crucial provision would shield companies from private lawsuits and antitrust laws if they seek help or cooperate with one another. Democrats had long resisted this legal safe harbor at the behest of plaintiffs lawyers who view corporate victims of cyber attack as another source of plunder.

The plaintiffs bar aside, the bill's main opponents now are big tech companies that are still traumatized by the fallout from the Edward Snowden data theft. Apple, Dropbox and Twitter, among others, say the bill doesn't do enough to protect individual privacy and might even allow government snooping.

Everyone knows government makes mistakes, but the far larger threat to privacy is from criminal or foreign-government hackers who aren't burdened by U.S. due-process protections. Cooperation is voluntary, and the bill includes penalties if government misuses the information. Before either side can share data, personal information that might jeopardize customer privacy must be scrubbed.

The tech giants are the outliers in this debate, while nearly all of the rest of American business supports the bill. The White House has said Mr. Obama will sign the legislation, which would make it a rare example of bipartisan cooperation. The security-privacy debate is often portrayed as a zero-sum tradeoff, but this bill looks like a win for both: Helping companies better protect their data from cyber thieves will enhance American privacy.

Mrs. FEINSTEIN. The first is from the Washington Post dated October 22, entitled ''The Senate should take a crucial first step on cybersecurity.'' The second is in today's Wall Street Journal, and it is entitled ''A Cyber Defense Bill, At Last: Data sharing can improve security and consumer privacy.''

I also note the endorsement from Secretary Jeh Johnson on October 22.

I have been privileged to work with our chairman. We have really tried to produce a balanced bill. We have tried to make it understandable to private industry so that companies understand it and are willing to cooperate. This bill will allow companies and the government to voluntarily share information about cyber threats and the defensive measures they might be able to implement to protect their networks.

Right now, the same cyber intrusions are used again and again to penetrate different targets. That shouldn't happen. If someone sees a particular virus or harmful cyber signature, they should tell others so they can protect themselves.

That is what this bill does. It clears away the uncertainty and the concerns that keep companies from sharing this information. It provides that two competitors in a market can share information on cyber threats with each other without facing anti-trust suits. It provides that companies sharing

cyber threat information with the government for cyber security purposes will have liability protection.

As I have said many times, the bill is completely voluntary. If a company doesn't want to share information, it does not have to.

Today, we will vote on up to seven amendments. As late as this morning, Senator BURR and I have been working to see if we can reach agreement to accept or voice vote some of them, and I hope these discussions will be successful. However, I remain in agreement with Chairman BURR that we will oppose any amendments that undo the careful compromises we have made on this bill. Over the past 10 months, we have tried to thread a needle in fact to draft a bill that as I said gives the private sector the insurances it needs to share more information while including privacy protections to make sure Americans' information is not compromised.

I see on the floor the ranking member of the Homeland Security and Governmental Affairs Committee, the distinguished Senator from Delaware, and I thank Senator CARPER for all he has done to help us and also to make what I consider a major amendment on this bill, which as you know has been accepted.

Several of today's amendments would undo this balance. Senators WYDEN, HELLER, and FRANKEN have amendments that would lead to less information sharing. Each of them would replace clear requirements that are now in the bill on what a company or a government must do prior to sharing information with a new subjective standard that would insert the concern of legal liability.

I would offer to work with these Senators and others as the bill moves forward and hopefully goes into conference to see if there is a way to achieve their goals without interfering with the bill's goal of increasing information sharing.

Senator LEAHY's amendment would similarly decrease the amount of sharing by opening up the chances of public disclosure through the Freedom of Information Act of cyber threats shared under this bill. While the bill seeks to share information about the nature of cyber threats and suggestions on how to defend networks, this information should not be made widely available to hackers and cyber criminals who could use it for their own purposes.

Senator BURR and I worked closely with Senators LEAHY and CORNYN in putting together the managers' package to remove a FOIA exemption that they viewed as unnecessary and harmful. I am pleased we were able to reach that agreement. However, the FOIA exemption that remains in the bill is needed to encourage companies to share this information, and I would oppose this amendment.

The President has an amendment on the other side of the spectrum which I will also strongly oppose. This amendment would basically undo one of the core concepts of this bill. Instead of requiring cyber information to go through a single portal at the Department of Homeland Security, it would allow companies to share cyber information directly with the FBI or the Secret Service and still provide full liability protection.

This change runs afoul of one of the most important privacy protections in the bill, which was to limit direct sharing of this cyber information with the intelligence community or with law enforcement. In other words, everything will go through the portal first, where it will receive an additional scrub to remove any residual personal information and then go to the respective departments. In this way the privacy is kept by not being able to misuse the authority to provide unrelated information directly to departments.

If there is a crime, companies should be able to share information with law enforcement—I agree with that—but that is not what this bill is about. This bill is about sharing cyber information on threats so there can be greater awareness and better defenses.

When there is a cyber crime and law enforcement is called in, we are talking about very different information. When the FBI investigates, it takes entire databases and servers. It looks at everything—far beyond the cyber information that could be lawfully shared in this act. So sharing with the FBI outside of the DHS portal may be appropriate in certain cases but not as a parallel option for cyber threat information.

In fact, our bill already makes clear in section 105(c)(E) that it ''does not limit or prohibit otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity.'' I would just refer to this chart which quotes section 105(c). It says exactly that.

This amendment would undo the key structure of this bill—the central portal for sharing information located at the Department of Homeland Security—and decrease the ability of the government to effectively manage all the cyber information it receives. So I will oppose this amendment and urge my colleagues to do the same.

I very much appreciate that the Senate will complete its consideration of this bill today. We still have a long way to go. We have to conference the House bill with our bill. I want to make this offer, and I know I think I speak for the chairman as well, that we are happy to work with any Member as we go into conference, but I hope we can complete these last few votes without upsetting the careful negotiations and compromise we have been able to reach.

Again, I thank the Chair.

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

The PRESIDING OFFICER. The Senator from Delaware.

Mr. CARPER. Let me start off by saying to Senator FEINSTEIN, 6 years ago, you, along with Senators SUSAN COLLINS, Joe Lieberman, Jay Rockefeller, and others started leading the effort to put in place comprehensive cyber security legislation and offered the first comprehensive bill dealing with information sharing. We had a vote in late 2012. It came up short, and we started all over again in the last Congress. You have shown great leadership right from the start. I thank you and I thank Senator BURR, the chair of the committee. I thank you for cooperating with us and with others to make sure that we have not just a good bill but a very good bill that addresses effectively the greatest challenges we face in our country.

I have heard Senator FEINSTEIN say this time and again, and I will say it again today: If companies don't want to share information with the Federal Government, they don't have to. It is elective. In some cases they can form their own groups called ISOCs that will share information with one another. They don't have to share information on attacks with the Federal Government. They can share it with other peers if they wish to, but if they do share it with the Federal Government, with a couple of narrow exceptions, we ask that it be shared with the Department of Homeland Security because the Department of Homeland Security is set up in large part to provide a privacy scrub.

Next month the DHS will have the ability, when these threat indicators come through that are reported by other businesses across the country, in real time to be able to scrub that information through the portal and remove from it personally identifiable information that should not be shared with other Federal agencies, and just like that, bingo, we are off to the races. It is a smart compromise that I am pleased and grateful to have worked out with Senators BURR and FEINSTEIN and their staff. I thank both their staff and ours as well.

The other piece is the legislation we literally took out of the Committee on Homeland Security and Governmental Affairs that has been pending. I think the entire title 2 of the managers' amendment is the legislation that Senator JOHNSON and I have worked on. We are grateful for that.

One piece of it is something called EINSTEIN 1, 2, and 3—not to be confused with the renowned scientist, Albert Einstein. But we have something called EINSTEIN 1, EINSTEIN 2, and EINSTEIN 3. What do they mean? What this legislation does is it means we are going to use these tools—we are going to continue to update and modernize these tools—to, No. 1, record intrusions; No. 2, to be able to detect the bad stuff coming through into the Federal Government; and No. 3, block it.

We are going to make sure it is not just something that is positive work on a piece of paper but that 100 percent of

the Federal agencies are able to use these new tools. Senator JOHNSON and I worked on legislation included in this package that uses encryption tools and doubles the number of processes we have available to better protect our information.

Finally, I would mention that Senator COLLINS, the former chair of the Homeland Security Committee—she and a number of our colleagues, including Senator MIKULSKI, Senator MCCASKILL, and others, have worked on legislation that we added to and all of that was reported out of the committee. All of this together is a very robust defender of our dot-gov domain and could be used to help those outside the Federal Government as well.

Going back to the last Congress, Tom Coburn and I worked together to do three things to strengthen the Department of Homeland Security to let it do its job. Growing up, I remember seeing cartoon ads in a magazine about some guy at the beach kicking sand on a smaller guy. The smaller guy in this case would have been the Department of Homeland Security, with respect to their ability to provide robust defense against cyber attacks. If I can use that cartoon as an analogy, in the past, the Department of Homeland Security was the 98-pound weakling, and it is no weakling anymore. Legislation that Dr. Coburn and I offered, passed in the Congress, to, No. 1, say the cyber ops center in the Department of Homeland Security is real. We are standing it up. We are making it real and robust.

The Federal Information Security Management Act for years was a paperwork exercise and was a once-a-year check to make sure our cyber defenses were secure. We are transforming that into a 24/7, robust, around-the-clock operation by modifying legislation and improving legislation called FISMA. We also in that legislation make clear what OMB's job is and we make clear what the job of the Department of Homeland Security is.

Finally, for years the Department of Homeland Security hired and trained cyber warriors, and just as they were getting really good, they were hired away because we couldn't retain them. We couldn't pay them or provide retention bonuses or hiring bonuses. We need to make sure we have some of the best cyber warriors in the world working at the Department of Homeland Security. Now DHS has that authority, and we will be able to hire these people.

Putting all this together, folks, what we have done is move the needle. With passage of this legislation we will move the needle and we need to do that.

There will be discussion later on of amendments. There are a couple of them that for this Senator are especially troubling. Senator FEINSTEIN has mentioned a couple of them, and I suspect Senator BURR has mentioned them as well. We will look at them as we go through, but a couple of them set this legislation back and I will very strongly oppose them.

Having said that, regarding the old saying—I am tired of hearing it and I am tired of saying it, but ''don't let the perfect be the enemy of the good.'' This isn't just good legislation, this is very good legislation, and it has gotten better every step of the way because of the willingness of the ranking member and the chairman of the Intel Committee to collaborate. The three C's at work are communicating, compromising, and collaborating. We should work out these amendments today and pass this bill.

I thank the Chair.

The PRESIDING OFFICER. The Senator from Nevada.

AMENDMENT NO. 2548, AS MODIFIED

Mr. HELLER. Mr. President, this Senator, like everyone else in this Chamber, realizes the need to address the threat of cyber attacks. The impact of these attacks is a matter of individual financial security as well as America's national security, and I contend that these efforts must not interfere with Americans' privacy. In doing so, the cure, which is this piece of legislation, is worse than the problem.

I have said it before and I will continue saying it, privacy for Nevadans is nonnegotiable. Nevadans elected me in part to uphold their civil rights and their liberties, and that is what I am on the floor doing today. That is why I fought for passage of the USA FREEDOM Act. That is why I offered my amendment being considered on this floor this given day. Hundreds of Nevadans have reached out to my office expressing concerns about the Cybersecurity Information Sharing Act, saying it did not do enough to safeguard their personal information.

Also tech companies, including Google, Apple, Microsoft, Oracle, and BSA Software Alliance, all expressed the same concerns about privacy under this piece of legislation. It is our responsibility in Congress to listen to these concerns and address them before allowing this piece of legislation to become law. I recognize the chairman of the intelligence committee does not support my amendment and has been encouraging our colleagues to oppose it.

With respect, however, I believe my amendment is a commonsense, middle-ground amendment. It ensures that we strike an appropriate balance that guarantees privacy, but also allows for real-time sharing of cyber threat indicators. My amendment would simply require the Federal Government, before sharing any cyber threat indicators, to strip out any personally identifiable information that they reasonably believe is not directly related to a cyber security threat.

This standard creates a wide protection for American's personal information. Furthermore, it also improves the operational capabilities of this cyber sharing program. DHS has stated that removing more personally identifiable information before sharing will help the private sector meaningfully digest that information as they work to combat cyber threats.

Again, I respect what Chairman BURR and Ranking Member FEINSTEIN are trying to do here, which is why I have carefully crafted this amendment to meet the needs of both sides—those fighting for privacy and those fighting for our national security. I would like to take a moment to address the concerns expressed by the chairman, who has argued that this amendment is a poison pill for this piece of legislation. I want to be clear: This amendment is not creating legal uncertainty that would delay the sharing of cyber threat indicators. In fact, the term ''reasonably believes'' is used as the standard for the private sector in the House-passed cyber bill. Let me repeat that. This phrase, ''reasonably believes,'' is the standard applied to the private sector in the House-passed bill. Our counterparts on the House Intelligence Committee felt that this standard was high enough to protect privacy while also meeting the goal of the bill which is real-time sharing.

If this standard is good enough for the private sector, it should be good enough for the Federal Government. Just 6 months ago, the chamber of commerce released a strong statement of support and praise for the House-passed cyber legislation. Not once did they release statements of concern over using the term ''reasonably believes'' as it applies to the private sector, the industry which they represent. I ask again: If it is good enough for the private sector, should it not be good enough for the Federal Government?

Finally, I am proud to have the support of two of the Senate's leading privacy advocates, Senators LEAHY and WYDEN, who have been fighting with me to make key changes to this bill to maintain Americans' rights. I strongly urge my colleagues today to vote in support of my simple fix. Let's keep our oath to the American people and make this bill stronger for privacy rights and civil liberties.

I yield the floor.

The PRESIDING OFFICER. The Senator from Oregon.

Mr. WYDEN. Mr. President, I ask unanimous consent that after Chairman BURR has spoken, I be recognized for 2 minutes.

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

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Mr. President, I want to say to my colleague Senator HELLER, I wish we could accommodate all of the amendments. The fact is that even a word here and there changes the balance of what Senator FEINSTEIN and I have tried to put together. Although on the surface it may not look like a big deal—I understand we have two competing bills that were passed in the House, and one has the language. The fact is, our language for the entirety of the bill does not match the House bill.

When you change something, we have to look at the cause and effect of it.

Here are the realities. This is a voluntary bill. I will start backward with some of the things Senator HELLER said. Technology companies are opposed to it. They are. I cannot do anything about that, but I can plead with them: Why would you deprive thousands of businesses that want to have a partnership with the Federal Government from having it because you have determined for your business, even though you are a large holder of personal data, that you don't want a partnership with the Federal Government.

I would suggest that the first day they get penetrated, they may find that partnership is worthy. I cannot change where they are on the legislation. The reality is that for a voluntary bill, it means there has to be a reason for people to want to participate. Uncertainty is the No. 1 thing that drives that away. We believe the change the Senator proposes provides that degree of uncertainty, and therefore we would not have information shared either at all or in a timely fashion. If it is not shared in a timely fashion, then we won't reach the real-time transfer of data which gives us the basis of minimizing data loss in this bill.

I think it is easy to look at certain pieces of the bill and say: Well, this does not change it that much. But it changes it in a way that would cause either companies to choose not to participate, or it may change it in a way that delays the notification to the Federal Government. Therefore, we are not able to accomplish what we set out to do in the mission of this bill, which is to minimize the amount of data that is lost not just at that company but across the U.S. economy.

Again, I urge our colleagues—we will move to amendments shortly. We will have an opportunity to debate for 1 minute on each side on those amendments. I would urge my colleagues to keep this bill intact. If we change the balance of what we have been able to do, then it changes the effects of how this will be implemented, and, in fact, we may or may not at the end of the day——

Mr. HELLER. Will the chairman yield time so I can respond to his comment?

Mr. BURR. I will be happy to yield.

Mr. HELLER. I appreciate everything the Senator is doing. I understand the importance of fighting against cyber attacks. I want to make two points—clarify two points that I think are very important. The language in this bill is the same standard the private sector is held to in the House-passed bill. The chamber had no problem 6 months ago when that bill was passed out of the House of Representatives.

So I continue to ask the question: If it is good enough—if this language is good enough for the private sector, why is it not good enough for the public sector, for the Federal Government? The second thing is that I believe my amendment does strike a balance, increasing privacy but still providing that real-time information sharing. I just wanted to make those two points.

Mr. BURR. Mr. President, I appreciate the Senator's input. I can only say to my colleagues that it is the recommendation of the vice chair and myself that this not be supported. It does change the balance, it puts uncertainty in the level of participation, and any delay from real time would, in fact, mean that we would not have lived up to the mission of this bill, which is to minimize data loss.

I think, though, that there are similarities between the House and Senate bills. Ours is significantly different, and therefore it has a different implication when you change certain words.

With that, I yield the floor.

The PRESIDING OFFICER. The Senator from Oregon.

Mr. WYDEN. Before he leaves the floor, I want to commend my colleague from Nevada. I strongly support his amendment.

AMENDMENT NO. 2621, AS MODIFIED

Colleagues, the first vote we will have at 11 o'clock is on my amendment No. 2621. This amendment is supported by a wide variety of leaders across the political spectrum, progressive voices that have focused on cyber security and privacy as well as conservative organizations. FreedomWorks, for example, an important conservative organization, announced last night that they will consider the privacy amendment that I will be offering. It will be the first vote, a key vote on their congressional scorecard.

It was the view of FreedomWorks that this amendment, the first vote, would add crucial privacy protections to this legislation. The point of the first amendment we will vote on is to strengthen privacy protections by requiring that companies make reasonable efforts to remove unrelated personal information about their customers before providing data to the government. It says that companies should take these efforts to the extent feasible. Let me say that this truly offers a great deal of flexibility and discretion to companies. It certainly does not demand perfection, but it does say to these companies that they should actually have to take some real responsibility, some affirmative step.

We will have a chance, I guess for a minute or so, when we get to the amendments, but for purposes of colleagues reflecting before we start voting, the first amendment I will be offering is backed by important progressive organizations, such as the Center for Democracy and Technology, and conservative groups, such as FreedomWorks, which last night said this is a particularly important vote with respect to liberty and privacy. It says that with respect to the standard for American companies, you just cannot hand it over, you have to take some affirmative steps—reasonable, affirmative steps—before you share personal information.

I yield the floor.

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Mr. President, we are going to go to these amendments, and we will have five amendments this morning and possibly up to five this afternoon starting at 4 o'clock.

AMENDMENT NOS. 2626, AS MODIFIED, AND 2557

I want to take this opportunity—there are two pending amendments that are not germane. I ask unanimous consent that it be in order to raise those points of order en bloc at this time.

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

Mr. BURR. I make a point of order that the Whitehouse amendment No. 2626 and the Mikulski amendment No. 2557 are not germane to amendment No. 2716.

The PRESIDING OFFICER. The points of order are well taken and the amendments fall.

Mr. BURR. Mr. President, I want to take this opportunity before we start the final process to thank the vice chairman. She has been incredibly willing to participate, even when we started in a different place than where we ended. She brought to the table a tremendous amount of experience on this issue because of the number of years she had worked on it. She was very accommodating on areas that I felt were important for us to either incorporate or at least debate.

What I really want to share with my colleagues is that we had a wholesome debate in the committee. The debate the vice chair and I and our staffs had was wholesome before it even came to the Presiding Officer or to Senator WYDEN. That is good. It is why some of the Members might have said in committee: Gee, this looks like a good amendment. Yet it did not fit within the framework of what the vice chair and I sat down and agreed to.

So this has been a process over a lot of months of building support, not just within this institution but across the country. It is not a process where I expected to get to the end and for there to be nothing but endorsements of the legislation. I have never seen a piece of legislation achieve that coming out of the Senate. But I think the vice chair and I believed when we actually put legislation together that we were on the same page. The fact is, it is important that today we are again still on the same page, that we have stuck there. I thank the vice chairman.

I also thank Senator JOHNSON and Senator CARPER, the chairman and the ranking member of the homeland security committee. They have been incredibly helpful and incredibly accommodating. We have tried to incorporate everything we thought contributed positively to this legislation, and they were huge contributors.

Lastly, let me say to all of my colleagues that it is tough to be put in a situation—the vice chair and myself—where we have Members on both sides

who are going to offer amendments—I understand that to them those amendments are very reasonable, and I would only ask my colleagues to understand the situation the vice chair and I are in. We have negotiated a very delicately written piece of legislation, and any change in that that is substantive we feel might, in fact, change the outcome of what this bill accomplishes.

We will have votes on amendments this morning. One of those amendments, Senator FLAKE's amendment—overnight we were able to negotiate a change in the sunset provision to 10 years. We will modify that on the floor and accept it by voice vote. The others will be recorded votes.

With that, I yield the floor.

AMENDMENT NO. 2621, AS MODIFIED

The PRESIDING OFFICER (Mrs. FISCHER). Under the previous order, the question occurs on amendment No. 2621, as modified, offered by the Senator from Oregon, Mr. WYDEN.

There is 2 minutes of debate equally divided.

The Senator from Oregon.

Mr. WYDEN. Madam President, virtually all agree that cyber security is a serious problem. Virtually all agree that it is useful to share information, but sharing information without robust privacy standards creates as many problems as it may solve.

The first amendment I am offering is supported by a wide variety of organizations across the political spectrum because they want what this amendment would do; that is, reasonable efforts have to be made to strike unrelated personal information before it is handed over to the government. Without that, you have a flimsy standard that says: When in doubt, hand it over.

I urge colleagues to support this amendment. It is backed by progressive groups and conservative groups.

Madam President, I ask unanimous consent to add Senator WARREN as a cosponsor to my amendment.

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

Mr. WYDEN. Madam President, I ask unanimous consent to have printed in the RECORD a letter of support from FreedomWorks, a leading conservative voice on these issues.

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

FREEDOMWORKS,
Washington, DC, October 26, 2015.

KEY VOTE YES ON THE WYDEN AMENDMENT #2621 TO CISA

As one of our over 6.9 million FreedomWorks activists nationwide, I urge you to contact your senators and ask them to vote YES on the Wyden amendment to add crucial privacy protections to the Cyber Information Sharing Act (CISA), S. 754.

CISA purports to facilitate stronger network security across the nation by facilitating the interchange of information on cyber threats between private companies and government agencies. But one of CISA's several gaping flaws is the incentive it creates for some companies to share this data recklessly.

The personally identifiable information (PII) of a company's users can be attached to cyber threat indicators after a hack—potentially sensitive information that is generally unnecessary to diagnose the threat. But since companies which share cyber threat data are completely immune to consequence if that shared data should be misused, their incentive is to share the data as quickly as possible—even if that means some would be sharing PII.

And if that personal data is irresponsibly shared with the government, it gets spread far and wide between government agencies (including the NSA) in real time, thanks to CISA's mandatory interagency sharing provision.

The Wyden amendment goes a long way toward addressing the potential misuse of this personal information by requiring companies which share cyber threat data to review said data to ensure that all PII that is not directly necessary to counter the cyber threat is deleted before it is shared.

Passing the Wyden amendment wouldn't fully fix the problems with CISA, but it is an important protection against potential distribution and misuse of innocent consumers' private information.

Please contact your senators and ask that they vote YES on the Wyden amendment to CISA. FreedomWorks will count the vote on this amendment as a Key Vote when calculating our Congressional Scorecard for 2015. The scorecard is used to determine eligibility for the FreedomFighter Award, which recognizes Members of Congress who consistently vote to support economic freedom and individual liberty.

Sincerely,

ADAM BRANDON,
CEO, FreedomWorks.

The PRESIDING OFFICER. The time of the Senator has expired.

The Senator from California.

Mrs. FEINSTEIN. Madam President, I rise to oppose the amendment. This amendment would replace a key feature of the underlying bill. Right now, under section 104(d) of the managers' amendment, a company is required to conduct a review of any information before it is shared and remove any personal information that is not ''directly related to a cybersecurity threat.''

Senator WYDEN's amendment, while well-intentioned, would replace that review with a requirement that a company must remove personal information ''to the extent feasible''—and there is the rub. This is a very unclear requirement. In this bill, we are trying to provide clarity on what a company has to do so that it is understandable. Companies understand what it means to conduct a review to see whether there is personal information and then strip it out. They don't know what may or may not be feasible, and they worry that this lack of clarity could create the risk of a lawsuit where the current language does not.

The PRESIDING OFFICER. The time of the Senator has expired.

Mrs. FEINSTEIN. Therefore, I ask my colleagues to join with me in voting no on the Wyden amendment.

The PRESIDING OFFICER. The question is on agreeing to the Wyden amendment, as modified.

Mr. BURR. Madam President, I ask for the yeas and nays.

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The clerk will call the roll.

The legislative clerk called the roll.

Mr. CORNYN. The following Senators are necessarily absent: the Senator from Texas (Mr. CRUZ), the Senator from Kentucky (Mr. PAUL), the Senator from Florida (Mr. RUBIO), and the Senator from Louisiana (Mr. VITTER).

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

The result was announced—yeas 41, nays 55, as follows:

[Rollcall Vote No. 285 Leg.]

YEAS—41

Baldwin	Gardner	Peters
Bennet	Gillibrand	Reed
Blumenthal	Heinrich	Reid
Booker	Heller	Sanders
Boxer	Hirono	Schatz
Brown	Klobuchar	Schumer
Cantwell	Leahy	Shaheen
Cardin	Lee	Stabenow
Casey	Markey	Sullivan
Coons	Menendez	Tester
Crapo	Merkley	Udall
Daines	Murkowski	Warren
Durbin	Murphy	Wyden
Franken	Murray	

NAYS—55

Alexander	Fischer	Moran
Ayotte	Flake	Nelson
Barrasso	Graham	Perdue
Blunt	Grassley	Portman
Boozman	Hatch	Risch
Burr	Heitkamp	Roberts
Capito	Hoeven	Rounds
Carper	Inhofe	Sasse
Cassidy	Isakson	Scott
Coats	Johnson	Sessions
Cochran	Kaine	Shelby
Collins	King	Thune
Corker	Kirk	Tillis
Cornyn	Lankford	Toomey
Cotton	Manchin	Warner
Donnelly	McCain	Whitehouse
Enzi	McCaskill	Wicker
Ernst	McConnell	
Feinstein	Mikulski	

NOT VOTING—4

Cruz	Rubio
Paul	Vitter

The amendment (No. 2621), as modified, was rejected.

AMENDMENT NO. 2548, AS MODIFIED

The PRESIDING OFFICER. Under the previous order, the question occurs on amendment No. 2548, as modified, offered by the Senator from Nevada, Mr. HELLER.

There is 2 minutes of debate equally divided.

The Senator from Nevada.

Mr. HELLER. Madam President, the chairman has stated that this piece of legislation has privacy protections. But I don't believe it goes far enough or we wouldn't be in this Chamber, vote after vote after vote, trying to move this so there is some personal privacy and so there are some liberties that are protected.

This amendment in front of us right now is a commonsense, middle-ground approach that strengthens the standards for the Federal Government removing personal information prior to sharing it with the private sector.

I want to leave my colleagues with two points. This is the same standard

that the private sector is held to in the House-passed bill, supported by the Chamber. If this amendment is good enough for the private sector, the question is, Why isn't it good enough for the Federal sector or the government? No. 2, my amendment strikes a balance between increasing privacy but still providing for real-time information sharing.

I urge my colleagues to support this amendment.

I yield the floor.

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Madam President, Senator FEINSTEIN and I have tried to reach a very delicate balance. We think we have done that. Senator HELLER raised one specific issue. He said the chamber is supportive of the language. Let me just read: The chamber opposes Senator HELLER's amendment for much of the same reason that we oppose comparable amendments being offered. It says: The difficulty with seemingly simple tweaks and wording is that interpreting the language, such as '' reasonably believes'' and ''reasonable efforts'' in legislation, is far from simple. It would create legal uncertainty and is contrary to the goal of real-time information sharing. The chamber will press to maintain NOS as the standard.

Hopefully, this shares some texture with my colleagues about how difficult this has been. As I said earlier, I would love to accept all of the amendments. But when it changes the balance of what we have been able to put—when we take a voluntary bill and provide uncertainty, we have now given a reason for either companies not to participate or for the government to delay the transmission to the appropriate agencies.

The PRESIDING OFFICER. The Senator's time has expired.

Mr. BURR. We believe we have the right protections in place. I urge my colleagues to defeat the Heller amendment.

The PRESIDING OFFICER. The question is on agreeing to the amendment, as modified.

Mr. THUNE. I ask for the yeas and nays.

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The clerk will call the roll.

The bill clerk called the roll.

Mr. CORNYN. The following Senators are necessarily absent: the Senator from Texas (Mr. CRUZ), the Senator from Kentucky (Mr. PAUL), the Senator from Florida (Mr. RUBIO), and the Senator from Louisiana (Mr. VITTER).

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

The result was announced—yeas 47, nays 49, as follows:

[Rollcall Vote No. 286 Leg.]

YEAS—47

Baldwin	Ernst	Menendez
Barrasso	Flake	Merkley
Bennet	Franken	Moran
Blumenthal	Gardner	Murkowski
Booker	Gillibrand	Murray
Boxer	Heinrich	Peters
Cantwell	Heitkamp	Portman
Cardin	Heller	Reed
Casey	Hirono	Sanders
Cassidy	Hoeven	Sullivan
Coons	Kaine	Tester
Crapo	Lankford	Toomey
Daines	Leahy	Udall
Donnelly	Lee	Warren
Durbin	Markey	Wyden
Enzi	McCaskill	

NAYS—49

Alexander	Grassley	Roberts
Ayotte	Hatch	Rounds
Blunt	Inhofe	Sasse
Boozman	Isakson	Schatz
Brown	Johnson	Schumer
Burr	King	Scott
Capito	Kirk	Sessions
Carper	Klobuchar	Shaheen
Coats	Manchin	Shelby
Cochran	McCain	Stabenow
Collins	McConnell	Thune
Corker	Mikulski	Tillis
Cornyn	Murphy	Warner
Cotton	Nelson	Whitehouse
Feinstein	Perdue	Wicker
Fischer	Reid	
Graham	Risch	

NOT VOTING—4

Cruz	Rubio
Paul	Vitter

The amendment (No. 2548), as modified, was rejected.

AMENDMENT NO. 2587, AS MODIFIED

The PRESIDING OFFICER. Under the previous order, the question occurs on amendment No. 2587, as modified, offered by the Senator from Vermont, Mr. LEAHY.

The Democratic leader.

Mr. REID. Madam President, I would ask that my remarks be under leader time.

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

CONGRATULATING SENATOR LEAHY ON CASTING HIS 15,000TH VOTE

Mr. REID. Mr. President, today my friend and colleague PAT LEAHY has reached another milestone in an extraordinary career. He just cast his 15,000th vote. That is remarkable. He is only the sixth Senator in the history of this great body to have done that. In 226 years, he is one of 6.

Today's momentous occasion should come as no surprise because his entire career in public service has been history in the making. He graduated from St. Michael's College, which is a Vermont institution. He graduated from Georgetown University Law Center.

He was first appointed as the State's attorney when he was 26 years old. He was then reelected on two separate occasions. During that time, PAT LEAHY was a nationally renowned prosecutor. In 1974—his last as a State's attorney—he was selected as one of the three most outstanding prosecutors in America.

At age 34, PAT became the first Democrat in U.S. history to be elected to the Senate from Vermont. After he was elected, the Republican Senator he was to succeed, George Aiken, was asked by some to resign his seat a day early—which you could do in those days—to give Senator LEAHY a head start in seniority among his fellow freshmen. Here is what Senator Aiken said: ''If Vermont is foolish enough to elect a Democrat, let him be number 100.''

Senator LEAHY's career has proven that the people of Vermont were wise in selecting him. From No. 100, Senator LEAHY over time ascended to the rank of President pro tempore of the Senate. Senator LEAHY has spent four decades in the Senate fighting for justice and equality. As the chairman of the Judiciary Committee, he became a national leader for an independent judiciary, the promotion of equal rights, and the protection of our Constitution.

His main focus, though, has always been Vermont. He carries with him a picture of what he calls his farmhouse, which is on lots of acres. It looks like a picture you would use if you were trying to get somebody to come and stay at your place—it is just beautiful. It doesn't remind me of the desert, but it is beautiful.

Over the years, he has done everything he can to protect the State's natural beauty, the resources, land and water, through conservation efforts. When people visit Vermont, they see these beautiful green vistas, pristine lakes and rivers, and picturesque farms. Senator LEAHY has worked hard to keep Vermont that way.

Senator LEAHY has done everything in his power to promote agriculture in his home State. As former chair of the agriculture committee, I can remember what he has done to protect the dairy industry. It is legend what he has done to protect the dairy industry. We all remember holding up the Senate for periods of time until he got what he wanted for dairy. He wrote the Organic Foods Production Act of 1990, which helped foster Vermont and America's growing organic food industry. Today, organic foods are a $40 billion industry. Many of those organic farms and businesses are based in Vermont.

After Tropical Storm Irene, I remember, graphically, his fighting for the State of Vermont. That storm devastated parts of Vermont. Roads were underwater for weeks. He helped secure $500 million in assistance for the people of Vermont to overcome a brutal natural disaster.

I am fortunate to be able to serve with PAT LEAHY here in the Senate. He is more than a colleague; he really is a dear friend, as is his wife of 52 years, Marcelle, whom Landra and I know well. We have helped each other through our times of joy and our times of travail. Senator LEAHY and his wife Marcelle have three wonderful children and five grandchildren. Give PAT a minute alone and he will start telling you about them.

Senator LEAHY, congratulations on your 15,000th vote in the U.S. Senate.

Mr. LEAHY. I thank my colleague.

(Applause, Senators rising.)

The PRESIDING OFFICER. The majority leader.

Mr. MCCONNELL. Madam President, as the Democratic leader has pointed out, this is indeed the 15,000th vote of the Senator from Vermont. That means he has taken the largest number of votes among all of us currently serving here in the Senate. It means he has taken the sixth largest number of votes in Senate history. It certainly means he has taken more votes than any other Senator from his State, and Vermont has been sending Senators here since the late 1700s.

That is not the only thing that sets him apart from every other Vermonter to serve here in the Senate. He was the first Democrat elected to serve from Vermont. Unfortunately, that is a habit that has not continued. I think we can safely assume he is Vermont's first Batman fanboy to serve as well; the first Bat fan and probably the first Dead Head as well.

There is no doubt that our colleague is the longest serving current Member of the Senate from any State. We are happy to recognize today his 15,000th vote.

(Applause, Senators rising.)

The PRESIDING OFFICER. The Senator from Iowa.

Mr. GRASSLEY. May I have 1 minute to speak to that point?

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

Mr. GRASSLEY. Madam President, I wish to commemorate my friend and colleague for casting his 15,000th vote today in the Senate.

Senator LEAHY has been a stalwart Member of this body since joining the Senate at the age of 34 in 1975. Four decades later, Senator LEAHY continues to serve his State and our Nation with great passion and conviction.

Senator LEAHY has been a good friend as we work together in leading the Senate Judiciary Committee.

So, Senator LEAHY, congratulations on this tremendous milestone. I hope we can cast many more votes together as we continue to work in a bipartisan way on the committee.

I applaud the Senator from Vermont for his great commitment to service, and I wish him many more votes in the future.

(Applause, Senators rising.)

The PRESIDING OFFICER. The junior Senator from Vermont.

Mr. SANDERS. Madam President, I rise to say a few words in congratulating Senator LEAHY, not just for his 15,000th vote but on his many years of service serving the people of the State of Vermont. Vermont is very proud of all of the work PAT LEAHY has done.

As we all know, Senator LEAHY has been a champion on agriculture issues, on protecting family farmers, especially in dairy and organics. He has been a champion in fighting for civil liberties in this country. He has been a champion on environmental issues, making sure the planet we leave our kids is a clean and healthy planet. He has been a champion on women's issues, and on so many other issues.

Senator LEAHY, on behalf of the people of Vermont, I want to thank you so much for your years of service.

(Applause, Senators rising.)

Mr. LEAHY. Madam President, I want to thank my dear friends, Senator REID, Senator MCCONNELL, Senator SANDERS, and Senator GRASSLEY for their comments, and I appreciate the opportunity to be able to serve with them. I thank the members of the Senate for this opportunity to make a very few observations about this personal milestone.

You know, the Senate offers both great opportunities and responsibility for both Senators from Vermont and all who serve here. We have a chance, day after day, to make things better for Vermonters and for all Americans. We can strengthen our country and ensure its vitality into the future. We can forge solutions in the unending quest throughout this Nation's history to form a more perfect Union.

I cast my first vote in this Chamber in 1975 on a resolution to establish the Church Committee. The critical issues of the post-Watergate era parallel issues we face today—proof of the enduring fact that, while the votes we cast today address the issues we face now, problems will persist, threats will continue, and improvements to the democracy we all revere can always be made.

I think back on the 15,000 votes I have cast on behalf of Vermonters. A lot of them come quickly to mind today—some specific to Vermont and some national and some global—writing and enacting the organic farm bill, the charter for what has become a thriving $30 billion industry; stronger regulations on mercury pollution and combating the effects of global warming; emergency relief for the devastation caused by Tropical Storm Irene; adopting price support programs for small dairy farmers; fighting for the privacy and civil liberties of all Americans; supporting the Reagan-O'Neill deal to save Social Security; nutrition bills to help Americans below the poverty line; bipartisan—strongly bipartisan—campaign reform in McCain-Feingold; the bipartisan Leahy-Smith Act, on patent reform; reauthorizing and greatly expanding and strengthening the Violence Against Women Act; opposing the war in Iraq, a venture that cost so many lives and trillions of taxpayer dollars.

The Senate at its best can be the conscience of the Nation. I have seen that when it happens, and I marvel in the fundamental soundness and wisdom of our system every time the Senate stands up and is the conscience of our Nation. But we cannot afford to put any part of the mechanism on automatic pilot. It takes constant work and vigilance to keep our system working as it should for the betterment of our society and the American people. And we can only do it if we work together.

I am so grateful to my fellow Vermonters for the confidence they have shown in me. It is a measure of trust that urges me on. I will never betray it, and I will never take it for granted. Reflecting on the past 15,000 votes reminds me about the significance every time we vote, why I feel energized about what votes lie ahead, and how we can keep making a difference.

I thank my friends, the two leaders, for their remarks, my respected Senate colleague, Senator SANDERS, my friend, Senator GRASSLEY, with whom I've served a long time. I appreciate my friendship with them and have appreciated my friendship with other leaders, including Senators Mansfield, Byrd, Baker, Dole, Lott, and Daschle, and lifelong gratitude to my former colleague, Senator Stafford, a Republican, who took me under his wing and guided me. And I am privileged to serve now—I mean, our whole Vermont delegation is here: Senator SANDERS, Congressman WELCH, and myself. Not many other States could do that and fit all of them in this body. And lastly I remember what a thrill it was to tell my wife, Marcelle, when I cast my first vote. And now 40 years later, I can still tell her about the 15,000th vote, and she knows, she and our children and grandchildren are the most important people in my life.

I do not want to further delay the Senate's work today, and I will reflect more on this milestone later. I thank you for your friendships that have meant more to me and my family than I can possibly say, and I look forward to continuing serving here. Thank you very, very much.

(Applause, Senators rising.)

Mr. DURBIN. Madam President, I want to add my voice to the well-deserved chorus of congratulations for our colleague and friend from Vermont.

Of the 1,963 men and women who have ever served in the U.S. Senate, only six have the distinction of casting 15,000 votes. And of those august six, only PATRICK LEAHY continues to serve in this body today. The only other members of the 15,000-vote league are Senators Robert C. Byrd, Strom Thurmond, Daniel Inouye, Ted Kennedy, and Ted Stevens.

More important than the number of votes Senator LEAHY has cast, however, is the wisdom and courage reflected in his votes.

He was elected to the U.S. Senate in 1974—part of an historic group of new Senators known as the ''Watergate Babies.''

He has voted time and again to uphold the values of our Constitution—even when it contained some political risk.

His very first vote in this Senate was to authorize the Church Committee—the precursor to today's Senate Select Committee on Intelligence. The Church Committee was created to investigate possible illegalities by the CIA, the FBI, and the National Security Agency—and it resulted in major reforms.

As you may know, Senator LEAHY is a major Batman fan. In fact, he has made several cameo appearances in Batman movies.

His affinity for the Caped Crusader makes sense. You see, Batman is one of the few superheroes with no superhuman powers. He is simply a man with unusual courage and determination to fight wrongdoing. That is PATRICK LEAHY, too.

I have served on the Senate Judiciary Committee for more than 18 years. During that time, Senator LEAHY has been either our committee chairman or its ranking member.

I have the greatest respect for his fidelity to the rule of law and his determined efforts to safeguard the independence and integrity of America's Federal courts.

He is a champion of human rights at home and abroad.

According to the nonpartisan website GovTrack, Senator LEAHY has sponsored more bipartisan bills than any other current member of this Senate. Sixty-one percent of his bills have had both Democratic and Republican cosponsors. In this time of increasingly sharp partisanship, that is a record that we would all do well to emulate.

I am particularly grateful to Senator LEAHY for his strong support of a bipartisan bill that I am cosponsoring, along with a broad array of Senators, from Chairman CHUCK GRASSLEY to Senator CORY BOOKER. The Sentencing Reform and Corrections Act would make Federal sentencing laws smarter, fairer, more effective, and more fiscally responsible. It passed the Judiciary Committee last week by a vote of 15–5. Senator LEAHY's leadership has been critical in building this broad support, and I look forward to the day—in the near future, I hope—when we can celebrate passage of this important measure.

I learned recently that Senator LEAHY dedicates all of his fees and royalties from his acting roles to charities. A favorite charity is the Kellogg-Hubbard library in Montpelier, VT, where he read comic books as a child. I hope that there are young boys and girls discovering in that library the same uncommon courage and love of justice that PATRICK LEAHY found there.

America needs more heroes like PAT LEAHY.

AMENDMENT NO. 2587, AS MODIFIED

The PRESIDING OFFICER. Under the previous order, the question occurs on amendment No. 2587, as modified, offered by the Senator from Vermont, Mr. LEAHY.

Mr. MCCONNELL. I ask for the yeas and nays.

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The yeas and nays were ordered.

There will now be 2 minutes equally divided.

The Senator from California.

Mrs. FEINSTEIN. Madam President, I rise regretfully to speak against the amendment directly following the important monument of 15,000 votes by one of the idols of my life, but so be it.

As it might become very clear, Senator BURR and I, on a bill that came out of committee 14 to 1, have tried to keep a balance and have tried to prevent this kind of information sharing from being a threat to business so they won't participate. Therefore, the words that are used are all important as to whether they have a legal derivation. Senator LEAHY's amendment would essentially decrease the amount of sharing by opening up the chance of public disclosure through the Freedom of Information Act of cyber threats shared under this bill.

Now, we seek to share information about the nature of cyber effects and suggestions on how to defend networks. This information clearly should not be made available to hackers and cyber criminals who could use it for their own purposes. So Senator BURR and I worked closely with Senator LEAHY and Senator CORNYN in putting together the managers' package to remove a FOIA exemption that they viewed as unnecessary and harmful. That has been removed in the managers' package.

The PRESIDING OFFICER. The time of the Senator has expired.

Mrs. FEINSTEIN. I thank the Chair.

The PRESIDING OFFICER. The Senator from Vermont.

Mr. LEAHY. Madam President, as much as I hate to disagree with my dear friend from California, I will on this amendment.

I don't like to see unnecessary exemptions to the Freedom of Information Act.

Today I offer an amendment to the Cybersecurity Information Sharing Act that would remove from the bill an overly broad and wholly unnecessary new FOIA exemption. That new exemption to our Nation's premier transparency law was added without public debate and in a closed session by the Senate Intelligence Committee. Any amendments to the Freedom of Information Act should be considered openly and publicly by the Senate Judiciary Committee, which has exclusive jurisdiction over FOIA—not in secret by the Senate Intelligence Committee.

I expect that much of the information to be shared with the government under CISA would be protected from disclosure to the general public. A thorough committee process, including consideration by the Senate Judiciary Committee, would have made clear that the vast majority of sensitive information to be shared under this bill is already protected from disclosure under existing FOIA exemptions. This includes exemption (b)(4), which protects confidential business and financial information; exemption (b)(6) which protects personal privacy; and exemption (b)(7), which protects information related to law enforcement investigations.

In case there is any doubt that this information would be exempt from disclosure, the underlying bill already makes clear that information provided to the Federal Government ''shall be considered the commercial, financial, and proprietary information'' of the entity submitting the information. Commercial and financial information is exempt from disclosure under FOIA pursuant to exemption (b)(4), and additional protections are unnecessary. The comprehensive exemptions already in law have been carefully crafted to protect the most sensitive information from disclosure while prohibiting the Federal Government from withholding information the public is entitled to. Creating unnecessary exemptions will call into question the existing FOIA framework and threaten its twin goals of promoting government transparency and accountability.

The new FOIA exemption in the cyber bill also includes a preemption clause that is overly broad and sets a terrible precedent. As drafted, it applies not only to FOIA, but to all State, local, or tribal disclosure laws. By its very terms, this provision applies not just to transparency and sunshine laws, but to any law ''requiring disclosure of information or records.'' Because this broad preemption of State and local law has not received careful, open consideration, there has not been adequate consultation with State and local governments to consider the potential impacts. Such a sweeping approach could impact hundreds of State and local laws and lead to unintended consequences.

Amending our Nation's premier transparency law and preempting State and local law deserves more public debate and consideration. If we do not oppose this new FOIA exemption, then I expect more antitransparency language will be slipped into other bills without the consideration of the Judiciary Committee. Just a few months ago, I was here on the Senate floor fighting against new FOIA exemptions that had been tucked into the surface transportation bill, and I have no doubt I will be down here again in the future fighting similar fights. But an open and transparent government is worth fighting for. I believe in transparency in our Federal Government, and I believe that FOIA is the backbone to ensuring an open and accountable government. I urge all Members to join me in this effort and vote for the Leahy amendment.

The PRESIDING OFFICER. The time of the Senator has expired.

Mr. LEAHY. I thank the Chair.

The PRESIDING OFFICER. The question is on agreeing to amendment No. 2587, as modified.

The yeas and nays have been ordered.

The clerk will call the roll.

The senior assistant legislative clerk called the roll.

Mr. CORNYN. The following Senators are necessarily absent: the Senator from Texas (Mr. CRUZ), the Senator from Kentucky (Mr. PAUL), the Senator from Florida (Mr. RUBIO), and the Senator from Louisiana (Mr. VITTER).

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

The result was announced—yeas 37, nays 59, as follows:

[Rollcall Vote No. 287 Leg.]

YEAS—37

Baldwin	Gillibrand	Reid
Bennet	Heinrich	Sanders
Blumenthal	Heller	Schatz
Booker	Hirono	Schumer
Boxer	Klobuchar	Shaheen
Brown	Leahy	Stabenow
Cantwell	Lee	Sullivan
Cardin	Markey	Tester
Casey	Menendez	Udall
Coons	Merkley	Warren
Daines	Murray	Wyden
Durbin	Peters	
Franken	Reed	

NAYS—59

Alexander	Fischer	Moran
Ayotte	Flake	Murkowski
Barrasso	Gardner	Murphy
Blunt	Graham	Nelson
Boozman	Grassley	Perdue
Burr	Hatch	Portman
Capito	Heitkamp	Risch
Carper	Hoeven	Roberts
Cassidy	Inhofe	Rounds
Coats	Isakson	Sasse
Cochran	Johnson	Scott
Collins	Kaine	Sessions
Corker	King	Shelby
Cornyn	Kirk	Thune
Cotton	Lankford	Tillis
Crapo	Manchin	Toomey
Donnelly	McCain	Warner
Enzi	McCaskill	Whitehouse
Ernst	McConnell	Wicker
Feinstein	Mikulski	

NOT VOTING—4

Cruz	Rubio
Paul	Vitter

The amendment (No. 2587), as modified, was rejected.

AMENDMENT NO. 2582

The PRESIDING OFFICER. Under the previous order, the question occurs on amendment No. 2582, offered by the Senator from Arizona, Mr. FLAKE.

The Senator from North Carolina.

AMENDMENT NOS. 2582, AS MODIFIED, AND 2552, AS FURTHER MODIFIED

Mr. BURR. Madam President, I ask unanimous consent that the Flake amendment No. 2582 and the Coons amendment No. 2552 be modified with the changes at the desk.

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

The amendments (No. 2582), as modified, and (No. 2552), as further modified, are as follows:

AMENDMENT NO. 2582, AS MODIFIED

At the end, add the following:

SEC. 11. EFFECTIVE PERIOD.

(a) IN GENERAL.—Except as provided in subsection (b), this Act and the amendments made by this Act shall be in effect during the 10-year period beginning on the date of the enactment of this Act.

(b) EXCEPTION.—With respect to any action authorized by this Act or information obtained pursuant to an action authorized by this Act, which occurred before the date on which the provisions referred to in subsection (a) cease to have effect, the provisions of this Act shall continue in effect.

AMENDMENT NO. 2552, AS FURTHER MODIFIED

Beginning on page 23, strike line 3 and all that follows through page 33, line 10 and insert the following:

(3) REQUIREMENTS CONCERNING POLICIES AND PROCEDURES.—Consistent with the guidelines required by subsection (b), the policies and procedures developed and promulgated under this subsection shall—

(A) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 104(c) through the real-time process described in subsection (c) of this section—

(i) are shared in an automated manner with all of the appropriate Federal entities;

(ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and

(iii) may be provided to other Federal entities;

(B) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 104 in a manner other than the real time process described in subsection (c) of this section—

(i) are shared as quickly as operationally practicable with all of the appropriate Federal entities;

(ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and

(iii) may be provided to other Federal entities;

(C) consistent with this title, any other applicable provisions of law, and the fair information practice principles set forth in appendix A of the document entitled ''National Strategy for Trusted Identities in Cyberspace'' and published by the President in April 2011, govern the retention, use, and dissemination by the Federal Government of cyber threat indicators shared with the Federal Government under this title, including the extent, if any, to which such cyber threat indicators may be used by the Federal Government; and

(D) ensure there are—

(i) audit capabilities; and

(ii) appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this title in an unauthorized manner.

(4) GUIDELINES FOR ENTITIES SHARING CYBER THREAT INDICATORS WITH FEDERAL GOVERNMENT.—

(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Attorney General and the Secretary of Homeland Security shall develop and make publicly available guidance to assist entities and promote sharing of cyber threat indicators with Federal entities under this title.

(B) CONTENTS.—The guidelines developed and made publicly available under subparagraph (A) shall include guidance on the following:

(i) Identification of types of information that would qualify as a cyber threat indicator under this title that would be unlikely to include personal information or information that identifies a specific person not directly related to a cyber security threat.

(ii) Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat.

(iii) Such other matters as the Attorney General and the Secretary of Homeland Security consider appropriate for entities sharing cyber threat indicators with Federal entities under this title.

(b) PRIVACY AND CIVIL LIBERTIES.—

(1) GUIDELINES OF ATTORNEY GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1), develop, submit to Congress, and make available to the public interim guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this title.

(2) FINAL GUIDELINES.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1) and such private entities with industry expertise as the Attorney General considers relevant, promulgate final guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this title.

(B) PERIODIC REVIEW.—The Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers and private entities described in subparagraph (A), periodically, but not less frequently than once every two years, review the guidelines promulgated under subparagraph (A).

(3) CONTENT.—The guidelines required by paragraphs (1) and (2) shall, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats—

(A) limit the effect on privacy and civil liberties of activities by the Federal Government under this title;

(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information or information that identifies specific persons, including by establishing—

(i) a process for the timely destruction of such information that is known not to be directly related to uses authorized under this title; and

(ii) specific limitations on the length of any period in which a cyber threat indicator may be retained;

(C) include requirements to safeguard cyber threat indicators containing personal information or information that identifies specific persons from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines;

(D) include procedures for notifying entities and Federal entities if information received pursuant to this section is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator;

(E) protect the confidentiality of cyber threat indicators containing personal information or information that identifies specific persons to the greatest extent practicable and require recipients to be informed that such indicators may only be used for purposes authorized under this title; and

(F) include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified and other sensitive national security information.

(c) CAPABILITY AND PROCESS WITHIN THE DEPARTMENT OF HOMELAND SECURITY.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the heads of the appropriate Federal entities, shall develop and implement a capability and process within the Department of Homeland Security that—

(A) shall accept from any entity in real time cyber threat indicators and defensive measures, pursuant to this section;

(B) shall, upon submittal of the certification under paragraph (2) that such capability and process fully and effectively operates as described in such paragraph, be the process by which the Federal Government receives cyber threat indicators and defensive measures under this title that are shared by a private entity with the Federal Government through electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems except—

(i) consistent with section 104, communications between a Federal entity and a private entity regarding a previously shared cyber threat indicator to describe the relevant cybersecurity threat or develop a defensive measure based on such cyber threat indicator; and

(ii) communications by a regulated entity with such entity's Federal regulatory authority regarding a cybersecurity threat;

(C) shall require the Department of Homeland Security to develop and implement measures to remove, through the most efficient means practicable, any personal information of or identifying a specific person not necessary to identify or describe the cybersecurity threat before sharing a cyber threat indicator or defensive measure with appropriate Federal entities;

(D) ensures that all of the appropriate Federal entities receive in an automated manner such cyber threat indicators as quickly as operationally possible from the Department of Homeland Security;

(E) is in compliance with the policies, procedures, and guidelines required by this section; and

(F) does not limit or prohibit otherwise lawful disclosures of communications, records, or other information, including—

(i) reporting of known or suspected criminal activity, by an entity to any other entity or a Federal entity;

(ii) voluntary or legally compelled participation in a Federal investigation; and

(iii) providing cyber threat indicators or defensive measures as part of a statutory or authorized contractual requirement.

(2) CERTIFICATION.—Not later than 10 days prior to the implementation of the capability and process required by paragraph (1), the Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities, certify to Congress whether such capability and process fully and effectively operates—

(A) as the process by which the Federal Government receives from any entity a cyber threat indicator or defensive measure under this title; and

(B) in accordance with the policies, procedures, and guidelines developed under this section.

(3) PUBLIC NOTICE AND ACCESS.—The Secretary of Homeland Security shall ensure there is public notice of, and access to, the capability and process developed and implemented under paragraph (1) so that—

(A) any entity may share cyber threat indicators and defensive measures through such process with the Federal Government; and

(B) all of the appropriate Federal entities receive such cyber threat indicators and defensive measures as quickly as operationally practicable with receipt through the process within the Department of Homeland Security.

(4) EFFECTIVE DATE OF CERTAIN PROVISION.—The requirement described in paragraph (1)(C) shall take effect upon the earlier of—

(A) the date on which the Secretary of Homeland Security determines that the Department of Homeland Security has developed the measures described in paragraph (1)(C); or

(B) the date that is 12 months after the date of enactment of this Act.

AMENDMENT NO. 2582, AS MODIFIED

Mr. FLAKE. Madam President, I thank the chair of the subcommittee and the vice chair, ranking member, for working on this. This was initially a 6-year sunset. This has been moved under the amendment to a 10-year sunset. I believe it is important, when we deal with information that is sensitive, to have a look back after a number of years to see if we have struck the right balance.

We have done that on other sensitive programs like this. I think it ought to be done here. I appreciate the work that Senators BURR and FEINSTEIN and my colleagues have put into this.

I urge support.

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Madam President, I thank my colleagues. We have agreed on this. We can hopefully do this by voice vote.

The PRESIDING OFFICER. If there is no further debate, the question is on agreeing to the amendment, as modified.

The amendment (No. 2582), as modified, was agreed to.

AMENDMENT NO. 2612, AS FURTHER MODIFIED

The PRESIDING OFFICER. Under the previous order, the question occurs on amendment No. 2612, as further modified, offered by the Senator from Minnesota, Mr. FRANKEN.

The Senator from Minnesota.

Mr. FRANKEN. Madam President, the Franken, Leahy, Durbin, and Wyden amendment addresses concerns raised by privacy advocates, tech companies, and security experts, including the Department of Homeland Security.

The amendment tightens definitions of the terms ''cyber security threat'' and ''cyber threat indicator,'' which are currently too broad and too vague, and would encourage the sharing of extraneous information—unhelpful information.

Overbreadth is not just a privacy problem; as DHS has noted, it is bad for cyber security if too much of the wrong kind of information floods into agencies.

My amendment redefines ''cyber security threat'' as an action that is at least reasonably likely to try to adversely impact an information system. It is a standard that tells companies what is expected of them and assures consumers that CISA imposes appropriate limits.

The PRESIDING OFFICER. The Senator's time has expired.

Mr. FRANKEN. Madam President, I ask unanimous consent for 20 more seconds.

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

Mr. FRANKEN. The amendment also tightens the definition of ''cyber threat indicator'' to avoid the sharing of unnecessary information. The amendment is intentionally modest. It makes only changes that are most needed for the sake of both privacy and security.

I urge my colleagues to support this amendment.

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Madam President, let me say to my colleagues, again, we are trying to change the words that have been very delicately chosen to provide the certainty that companies understand and need for them to make a decision to share.

Like some other amendments, if you don't want them to share, then provide uncertainty. That is in language changing from ''may'' to ''reasonably likely,'' changing from ''actual'' or ''potential'' to ''harm caused by an incident.'' The Department of Homeland Security is for this bill. The White House is for this bill. Fifty-two organizations representing thousands of companies in America are for this bill. We have reached the right balance. Let's defeat this amendment and let's move to this afternoon's amendments.

I yield the floor.

The PRESIDING OFFICER. The question is on agreeing to the amendment, as further modified.

Mr. TILLIS. I ask for the yeas and nays.

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The clerk will call the roll.

The bill clerk called the roll.

Mr. CORNYN. The following Senators are necessarily absent: the Senator from Texas (Mr. CRUZ), the Senator from South Carolina (Mr. GRAHAM), the Senator from Kentucky (Mr. PAUL), the Senator from Florida (Mr. RUBIO), and the Senator from Louisiana (Mr. VITTER).

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

The result was announced—yeas 35, nays 60, as follows:

[Rollcall Vote No. 288 Leg.]

YEAS—35

Baldwin	Gillibrand	Peters
Bennet	Heinrich	Reid
Blumenthal	Heller	Sanders
Booker	Hirono	Schatz
Boxer	Klobuchar	Schumer
Brown	Lankford	Shaheen
Cantwell	Leahy	Stabenow
Cardin	Lee	Tester
Coons	Markey	Udall
Daines	Menendez	Warren
Durbin	Merkley	Wyden
Franken	Murray	

NAYS—60

Alexander	Collins	Grassley
Ayotte	Corker	Hatch
Barrasso	Cornyn	Heitkamp
Blunt	Cotton	Hoeven
Boozman	Crapo	Inhofe
Burr	Donnelly	Isakson
Capito	Enzi	Johnson
Carper	Ernst	Kaine
Casey	Feinstein	King
Cassidy	Fischer	Kirk
Coats	Flake	Manchin
Cochran	Gardner	McCain

McCaskill	Portman	Shelby
McConnell	Reed	Sullivan
Mikulski	Risch	Thune
Moran	Roberts	Tillis
Murkowski	Rounds	Toomey
Murphy	Sasse	Warner
Nelson	Scott	Whitehouse
Perdue	Sessions	Wicker

NOT VOTING—5

Cruz	Paul	Vitter
Graham	Rubio	

The amendment (No. 2612), as further modified, was rejected.

The PRESIDING OFFICER. The Senator from Missouri.

Mr. BLUNT. Madam President, I ask unanimous consent to address the floor for up to 15 minutes.

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

Mr. BLUNT. Madam President, last week I came to the floor to express my support for the Cybersecurity Information Sharing Act, which we are dealing with today. The bipartisan vote of 83 to 14 that happened later that day was an important step in the right direction to deal with this issue. The debate has been encouraging. We need to deal with this threat to our economy. It is a threat to our security, it is a threat to our privacy, and we need to deal with it now.

As I and others have said before, if we wait until there is an event that gets people's attention in such a dramatic way that everybody suddenly realizes what is at stake, there is no telling what kind of overreaction Congress will make. This has been a good debate at the time we should have it. Now, of course, we need to move on.

There have been a lot of amendments offered. Many amendments have been accepted by the managers of the bill. With almost all certainty, today we will finish the remaining amendments pending on the bill and hopefully finish the bill itself. A lot of these amendments have been very well-intentioned—in fact, I suspect they all have been well-intentioned—but in many cases they fundamentally undermine the core purpose of the bill, which is to have voluntary real-time sharing of cyber threats, to allow that sharing to be between private entities and the Federal Government, and even for private entities to be able to share with each other.

This is a bill that creates the liability protections and the anti-trust protections which that particular kind of sharing would allow. Of course, throughout this whole debate, there has been much discussion about how we protect our liberty in an information age. How do we have both security and liberty?

Having served for a number of years on both the House Intelligence Committee and the Senate Intelligence Committee, having served on the Armed Services Committee in the last Congress and in this Congress on the Defense Appropriations Committee, there is no argument in any of those committees that one of our great vulnerabilities is cyber security and how we protect ourselves.

We saw in the last few days that the head of the CIA had his own personal account hacked into apparently by a teenager who is in the process of sharing that information. If the head of the CIA and the head of Homeland Security do not know how to protect their own personal information, obviously information much more valuable than they might personally share is also in jeopardy.

We do need to ensure that we protect people's personal liberties. We need to do that in a way that defends the country. Both of those are primarily responsibilities that we accept when we take these jobs, and it is certainly our responsibility to the Constitution itself.

I think Chairman BURR and Vice Chairman FEINSTEIN have done a good job of bringing that balance together. This bill is carefully crafted in a way that creates a number of different layers of efforts to try to do both of those things.

First, the bill only encourages sharing; it doesn't require it. It doesn't require anybody to share anything they don't want to share, but it encourages the sharing of cyber threats. It works on the techniques and the malware used by hackers. It specifically does not authorize the sharing of personal information, and in fact the bill explicitly directs the Federal Government to develop and make available to the public guidelines to protect privacy and civil liberties in the course of sharing the information.

The Attorney General is required to review these guidelines on a regular basis. The bill mandates reports on the implementation and any privacy impacts by inspectors general and by the Privacy and Civil Liberties Oversight Board, to ensure that these threats to privacy are constantly looked at.

Senator FLAKE's amendment, which we accepted as part of the bill just a few minutes ago, guarantees that this issue has to be revisited.

I gave a speech at Westminster College in Fulton, MO, about a month ago at the beginning of the 70th year of the anniversary of Winston Churchill giving the ''Iron Curtain'' speech on that campus and talking about liberty versus security there. I said I thought one of the things we should always do is have a time that forced us as a Congress to revisit any of the laws we have looked at in recent years to be sure we protect ourselves and protect our liberty at the same time. This is a voluntary bill. Maybe that wouldn't have been quite as absolutely necessary here, but I was pleased to see that requirement again added to this bill, as it has been to other bills like this.

This is a responsible bill. The people the Presiding Officer and I work for can feel good about the responsible balance it has. It defends our security, but it also protects our liberty. I look forward to its final passage today. The debate would lead me to believe, and the votes would lead me to believe, that is going to happen, but of course we need to continue to work now to put a bill on the President's desk that does that.

There still remain things to be done. One of the things I have worked on for the last 3 years—Senator CARPER and I have worked together, Senator WARNER has been very engaged in this discussion, as has Chairman THUNE—is the protection of sensitive personal information as well as how do we protect the systems themselves.

Clearly this information sharing will help in that fight. There is no doubt about that. In addition to supporting this bill, I want to continue to work with my colleagues to see that we have a way to notify people in a consistent way when their information has been stolen.

There are at least a dozen different State laws that address how you secure personal information, and there are 47 different State laws that address how you tell people if their information has been stolen. That is too much to comply with. We need to find one standard. This patchwork of laws is a nightmare for everybody trying to comply and frankly a nightmare for citizens who get all kinds of different notices in all kinds of different ways.

Without a consistent national standard pertaining to securing information, without a consistent national standard pertaining to what happens when you have a data breach and your information is wrongly taken by someone else, we have only done part of this job. So I want us to continue to work to find the solutions there. We need to find a way to establish that standard for both data security and data breach. I am going to continue to work with the Presiding Officer and my other colleagues. Our other committee, the commerce committee, is a critical place to have that happen. I wish we could have done this on this bill. We didn't get it done on this bill, but I would say that now the first step to do what we need to do is dealing with the problem of cyber security in the way this bill does and then finish the job at some later time.

So I look forward to seeing this bill passed today. I am certainly urging my colleagues to vote for it. I think it has the protections the people we work for would want to see, and I am grateful to my colleagues for giving me a few moments here to speak.

I yield the floor.

RECESS

The PRESIDING OFFICER. Under the previous order, the Senate stands in recess until 2:15 p.m.

Thereupon, the Senate, at 1:01 p.m., recessed until 2:15 p.m. and reassembled when called to order by the Presiding Officer (Mr. PORTMAN).

CYBERSECURITY INFORMATION SHARING ACT OF 2015—Continued

The PRESIDING OFFICER. Under the previous order, the time until 4