United States of America

Congressional Record

PROCEEDINGS AND DEBATES OF THE 114th CONGRESS, FIRST SESSION

Vol. 161 WASHINGTON, TUESDAY, OCTOBER 27, 2015 No. 158

Senate

The Senate met at 10 a.m. and was called to order by the President pro tempore (Mr. HATCH).

PRAYER

The Chaplain, Dr. Barry C. Black, offered the following prayer:

Let us pray.

Sovereign Lord, we have heard of Your greatness from generation to generation. You sit enthroned in majesty, for Your glory covers all the Earth.

Today, bless and sustain our lawmakers and their staffs. May their words and deeds honor You. Lord, guide them in righteous paths that will keep America strong. Equip them to conduct the work of freedom with justice and humility. Give them contentment that comes from knowing and serving You.

Guide America, making it a lighthouse for a dark and turbulent world. Lord, thank You for being our strength and shield.

We pray in Your great Name. Amen.

PLEDGE OF ALLEGIANCE

The President pro tempore led the Pledge of Allegiance, as follows:

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

RECOGNITION OF THE MAJORITY LEADER

The PRESIDING OFFICER (Mr. COTTON). The majority leader is recognized.

FISCAL AGREEMENT AND CYBERSECURITY INFORMATION SHARING BILL

Mr. MCCONNELL. Mr. President, as colleagues have no doubt already noted, a fiscal agreement has been filed that addresses a number of important issues. Members currently have the opportunity to review it. I hope they will take that opportunity. I will certainly have more to say on the matter later. But for now, I encourage all our colleagues to examine the agreement.

On the legislation before the Senate today, the challenges posed by cyber attacks are real and they are growing. They don't just threaten governments and businesses; they threaten individuals as well. Everyone understands that a cyber attack can be a deeply invasive attack on personal privacy. Everyone understands that a cyber attack can be financially crippling. That is why everyone should want to see the bipartisan cyber security bill before us pass today.

Its voluntary information sharing provisions are key to defeating cyber attacks and protecting the personal information of the people we represent. We also know the bill contains measures to protect civil liberties and individual privacy.

It is no wonder the Senate voted to advance it by a large bipartisan vote of 83 to 14 last week. I want to thank Chairman BURR and Vice Chairman FEINSTEIN of the Intelligence Committee for their continued hard work on this legislation. We will consider a number of amendments from both sides of the aisle today. Then we will proceed to a final vote on the underlying bill. I urge every colleague to join me in voting to protect the personal data, privacy, and property of the American people.

ENERGY REGULATIONS

Mr. MCCONNELL. Mr. President, on one final matter, the Obama administration recently published massive energy regulations that will not do a thing to meaningfully affect global carbon levels. It will not make a noticeable difference to the global environment. But it will ship more middle-class jobs overseas. It will punish the poor. It will make it even harder for coal families in States such as Kentucky to put food on the table. In other words, it is facts-optional extremism wrapped in callous indifference. Senators from both parties are saying: Enough is enough.

We filed bipartisan measures that would allow Congress to overturn these two-pronged regressive regulations. I joined Senator HEITKAMP and Senator CAPITO on a measure that would address the prong that pertains to the existing energy sources. Senator MANCHIN joined me as I introduced a measure that would address the prong that pertains to new energy sources. Together these measures represent a comprehensive solution. Colleagues will join me to speak about these resolutions later today. I am sure they will say more about the measures we filed and the process associated with them.

But what everyone should know is this: The publication of these regulations does not represent an end but a beginning. It is the beginning of a new front to defend hard-working middle-class Americans from massive, massive regulations that target them. That front is opening here in Congress, and it is opening across the country as States file lawsuits and Governors stand up for their own middle-class constituents. The battle may not be short, and the battle may not be easy, but Kentuckians and hard-working Americans should know that I am going to keep standing up for them throughout this effort.

RECOGNITION OF THE MINORITY LEADER

The PRESIDING OFFICER. The Democratic leader is recognized.

BUDGET AGREEMENT

Mr. REID. Mr. President, Democrats have long called for bipartisan action to stop these devastating sequester cuts because they hurt our middle class

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

Printed on recycled paper.

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

p.m. is equally divided in the usual form.

The Senator from Rhode Island.

Mr. REED. Mr. President, I wish to comment briefly on the Cybersecurity Information Sharing Act that the Senate is considering. Let me first commend the sponsors, Senator BURR and Senator FEINSTEIN, for their extraordinary work.

This bill will help ensure greater sharing of cyber threat information, more rapidly and broadly, across industry and government. As we have seen with large-scale attacks against the Federal Government and companies such as Sony, there is an urgent need to start addressing these breaches. While such legislation is not going to eliminate our cyber security challenges, it should materially help to defeat and deter cyber attacks and assist law enforcement in tracking down and prosecuting cyber criminals. Information sharing will also assist the intelligence agencies and law enforcement to detect and trace the attacks originating from foreign actors, which is a crucial step in holding other countries accountable.

Many of our citizens and corporations are understandably concerned about the impact of information sharing on privacy. But we also must recognize that rampant cyber crime is a monumental threat to the privacy of the American people, and that sharing information about these criminal acts cannot only protect privacy but also protect our public safety and national security.

With respect to the specific privacy protections in the legislation before us, the managers of this bill have come a long way toward improving the balance between security and privacy protection, especially the changes made to the base bill by the managers' substitute.

A major area of concern was whether the government should be authorized to use information shared under this bill to investigate or prosecute a host of crimes unrelated to cyber security. Now the bill is more narrowly tailored and focused on using information gathered under this bill to go after crimes that are specifically related to cyber security.

The managers' substitute also adds a requirement that the information sharing procedures, required to be issued under this bill, include a duty to notify individuals when the Federal Government shares their personally identifiable information, or PII, erroneously.

The managers' substitute also includes an improved reporting requirement that will show the number of notices sent because the government improperly shared an individual's PII and the number of cyber threat indicators shared automatically and, in addition, the number of times these indicators were used to prosecute crimes.

So the managers' substitute has come a long way toward being more protective of individual privacy, and I would like, once again, to recognize Senators FEINSTEIN and BURR's hard work here and their willingness to listen to their colleagues. While I might personally have set the balance slightly different in some places, which is why I have supported some of the amendments before us, I think they have done a significant job in improving the bill and providing privacy protection.

I do want to draw my colleagues' attention to one important additional fact here, which in some cases has been largely overlooked. The cyber information sharing system established by this bill will require Federal dollars to implement. Many of the agencies involved—the Department of Homeland Security being the primary portal for shared threat indicators—are funded on the nondefense discretionary side of the ledger. This is an example of why I and many of my colleagues have been urging for sequester relief for both defense and nondefense spending—because we cannot defend our homeland without funding nondefense agencies such as the Department of Homeland Security and a host of other key Federal agencies. Indeed, I am encouraged that we are close to voting on a budget solution that will provide 2 years of sequester relief on a proportionally equal basis for defense and nondefense spending, and that protects the full faith and credit of the United States by taking the threat of default off the table until March of 2017.

For this reason, I look forward to final passage of this legislation. I once again commend the principal authors, Senator BURR and Senator FEINSTEIN, for their extraordinary effort.

I yield the floor.

The PRESIDING OFFICER. The Senator from Delaware.

AMENDMENT NO. 2581, AS MODIFIED

Mr. CARPER. Mr. President, I want to go back in time a little more than 12, 13 or 14 years ago, to 9/11. One of the lessons learned by the committee on which the Presiding Officer and I serve, now the Homeland Security and Governmental Affairs Committee, was learned from former Governor Tom Kean of New Jersey, cochair, along with former Congressman Lee Hamilton from Indiana, former chair of the House Foreign Affairs Committee. They were the cochairs of the 9/11 Commission. One of the things they brought to our committee and to the Congress, after a lot of work by a number of good men and women who served on that commission, was the root causes for how that disaster occurred: How could those four aircraft take down the Twin Towers, crash into the Pentagon, and crash into a field in Shanksville, PA, instead of this building right here? How could that have happened?

There are a number of reasons why it happened. But one of the reasons why it happened is that we had stovepiped our intelligence services. What the folks over at the FBI knew wasn't necessarily known or shared with the Department of Homeland Security. What the folks at the National Security Agency knew was not shared with either of the other two agencies. What the Defense Information Agency knew or what other agencies knew simply didn't get shared—stovepiped—because we did a lousy job of sharing the real story, the full truth on what was being plotted, what was going to come down and literally take thousands of lives in one day and change in many ways our country—in profound ways that still exist today. ''Stovepiping''—I have heard that word a hundred times in hearings and before our committee and in talking to folks in the 9/11 Commission. The legislation that we passed on the heels of that disaster was designed to make sure we didn't end up stovepiping again with intelligence information that might lead us to avert that kind of disaster. So far, it seems to be working and is much needed, and I think it has been helpful.

Today, I want to talk about a different kind of stovepiping that I am afraid we may end up with—not to avert or block an aviation takeover of an aircraft and disasters involving the aviation sector but a disaster in cyber space in the face of cyber threats to our country.

We are working here today and will be voting later today on an amendment or two and then on final passage of the Cybersecurity Information Sharing Act. Again, just to remind everybody, the reason why we are considering this is there needs to be a better sharing of information when businesses come under cyber attack from those within our country, outside of our country, cyber nations, and criminal organizations. We need to do a better job of sharing that information—business to business and business to government—and for the government to share that information within the government to agencies that need to know so we can respond to those attacks.

Shortly after the 9/11 Commission recommendations were enacted, one of the things that we did was we stood up a new department called the Department of Homeland Security. It is a civilian agency, as we know. It is not the Department of Defense. It is not the Department of Justice. It is not the FBI, and it is not the National Security Agency. It is a civilian organization.

When the Department of Homeland Security was created, one of the ideas behind it was that it would not be just a civilian operation, but it would be a civilian operation that could receive, from businesses and from other governmental entities, information relating to cyber attacks. That information could come through a portal—think about it; almost like a window—through which those threat indicators would be reported. Those threat indicators would come through that portal at the Department of Homeland Security. The Department of Homeland Security

would do, almost in real time, a privacy scrub to strip off from the information—the threat indicators submitted from other businesses or other government entities—Social Security numbers or other personally identifiable information or information that just shouldn't go to other Federal agencies or other businesses. They would strip it out—not in a week, not in a day, not in an hour, not even, in many cases, in a minute, but just like that—immediately—real-time privacy scrub.

As the Presiding Officer knows, we tried for years to be able to enact legislation that incentivizes businesses that have been victims of cyber attacks to share that information with one another, with other businesses, and with the Federal Government. A bunch of them have been reluctant to do it. Some of them have been reluctant to do it because they don't want to get sued. If they disclose that they had a breach and maybe their competitors didn't, how would that be used against them? How could they be named in lawsuits if attacks occurred?

So in order to get them to be willing to share information, we had to incent them. And the way we decided to incent them is to say: Share the information. You don't have to worry if you share it with the Department of Homeland Security through the portal established in this civilian agency. Share it with the Department of Homeland Security, and you have liability protection or, as it turns out, if you already shared it previously, if it has been shared previously with the Federal Government, you can share it again and still enjoy liability protection. You can share it with companies that are victims of cyber attacks, share it with their regulator, and still enjoy liability protection.

What we want to do is to make sure companies and businesses that are hacked don't just sit on the information, that they do something with it. This is a saying we have on Amtrak: If you see something, say something. If something happens to a business—a cyber attack intrusion—we want them to share it so other businesses and other Federal agencies can be prepared for it, look out for it, and stop it.

Where does this take me? This takes me to an amendment that we are going to be voting on later this afternoon offered by one of our colleagues, Senator COTTON. It would, I fear, risk revisiting stovepiping—not the kind of stovepiping that led to the disaster of 9/11 but stovepiping that could lead to cyber threats—threat indicators shared with the Federal Government but not with the Department of Homeland Security, which receives these threats and immediately disburses them to other agencies that have a need to know. But what the Cotton amendment would do is that it would say that a business that is a victim of a cyber attack could share with the FBI, could share with Secret Service, but wouldn't have to share with the Department of Homeland Security.

The reason why in our legislation, which Senator BURR, Senator FEINSTEIN, I, and others have worked on, we have it going through the Department of Homeland Security is because, more than any Federal agency, they are set up to do privacy scrubs. That is one of the things they do, and, frankly, they do it really well. Their job is to then spread that information and share that information back to the private sector, in some cases, and in other cases, just with relevant agencies—NSA, FBI, Department of Justice, Treasury, whoever else needs to know that information.

As part of the authors of the legislation, I join them in this. Our fear is if the information isn't shared with the Department of Homeland Security, which will then broadly share it in real-time and share that information with those who need to know it, and if it ends up that the FBI or, frankly, any other agency that doesn't have that ability to do a great privacy scrub maybe, that doesn't have maybe the mission to immediately share that information in real time to other relevant players, then the news—the word about that cyber attack—could literally stay at that agency—the FBI or the Secret Service, for that matter. We don't want that to happen. We don't want to see that information stovepiped in one agency. We want to make sure that it goes to one agency that does the privacy scrub. We want to make sure the agency that does the privacy scrub shares that information in real time with relevant Federal agencies and the private sector.

I probably shouldn't pretend to speak for Senator FEINSTEIN and Senator BURR. They will be here to speak for themselves. But I know they share my concerns about this legislation. I ask, on behalf of them, and, frankly, for others of us who believe that this is a dangerous amendment—and I don't say that lightly. We have worked really hard. We have worked really well across the aisle—literally for months now—to get to this point. To use a football analogy, we are not just in the red zone passing this legislation; we are on the 10-yard line, and it is first down and goal to go. Let's not muff the play. Let's get the ball to the end zone. Let's pass this legislation. Let's vote down the Cotton amendment, and let's go to conference. Let's go to conference and provide the kind of protection against cyber attacks that this country desperately needs and deserves.

I yield the floor.

The PRESIDING OFFICER. The Senator from West Virginia.

CARBON REGULATIONS

Mrs. CAPITO. Mr. President, today I rise on behalf of West Virginian workers, families, communities, and all hardworking Americans who will bear the burden of these onerous carbon mandates. The bipartisan resolution of disapproval, which I have introduced with my colleague Senator HEIDI HEITKAMP from North Dakota and 47 other cosponsors, will block EPA's greenhouse gas regulation targeting existing power sources. I also strongly support Leader MCCONNELL's companion resolution to block the regulations targeting new power limits.

As I was thinking about the speech today and as I rise to give this speech, I realize I have said many of these same words so many times before. I have expressed the same frustrations and spouted off similar statistics. What is the difference this time? The difference is we have already seen the devastating effects and the callous nature of regulatory overreach. We know what the new reality would be. The new reality would be what we are facing with these new carbon regulations: the reality of the families, the faces, and the hardships that we have already endured; the thousands of layoffs in my State of West Virginia that have already been issued; the jobs that have been lost and will never come back.

Just this morning, nearly 200 West Virginia coal miners in Randolph County were informed that their jobs will be gone by Christmas. Think about how those families will spend their Christmas holiday. Then consider how those realities will be magnified and felt throughout many households across the country if these carbon mandates move forward—the higher electricity bills that will result, the squeeze that already is squeezing struggling middle-class families who are living on fixed incomes, and the squeeze that those who live on fixed incomes will feel. Our most vulnerable will bear the burden. Consider the far-reaching effects these regulations will have on schools that are now seeing their budgets shrink, home values that are now on the decline, and fewer dollars that are available for public safety and law enforcement.

It is reality that the policies emanating from this government—from our government—are causing this destruction. This is not a natural disaster. This is not a fiscal crisis. This is not an uncontrollable event but a carefully crafted, precise, and very meditated assault on certain areas of the country. These are policies that help some States and truly hurt others, policies that target States like West Virginia and North Dakota where we produce some of the most reliable and affordable energy, and policies that are ripping the American dream away from families in my State and communities. Our families want and deserve healthy, clean air and water, and they want to live in a great environment. But policies from Washington that pit one State against another and prioritize certain communities and certain jobs over others are bringing the livelihoods of many to a halt. On behalf of Americans across the country, Members of Congress now have the opportunity to express our concerns with these carbon mandates. We have an opportunity to weigh in about whether these burdensome regulations should go into effect.

I believe that a majority of my colleagues understand the need for affordable and reliable energy, and that is why I am confident that Congress will pass these resolutions and place this critical issue of America's economic future squarely on President Obama's desk. With the international climate negotiations in Paris scheduled for December, the world is watching whether the United States will foolishly move forward with regulations that will do virtually nothing to protect our environment and will tie one hand behind our back economically. Even if the President vetoes these resolutions—and we recognize the likelihood that he will—passing them will send a clear message to the world that the American people do not stand behind the President's efforts to address climate change with economically catastrophic regulations.

I am pleased to be joined by several colleagues on the floor who understand the need for affordable and reliable energy. I would like to recognize Senator HEITKAMP.

I ask unanimous consent to engage in a colloquy with my colleagues for up to 30 minutes.

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

Ms. HEITKAMP. Thank you, Mr. President, and thank you to my great colleague from the great State of West Virginia, a State that has been powering America for many years—in fact, from the very beginning. My thanks go to all of the great workers and coal miners in her State who have added to our economic opportunity, not just for the people in West Virginia but for the people of an entire region.

That is one thing we forget—that in America a great miracle happens every day. We turn on a light switch and the lights come on. If that doesn't happen or if it is too expensive to turn on that light switch, we will not be the country that we are. With this regulation, I think what we have done is cede the all-important role of electrical security and energy security to an environmental agency that does not have the experience or expertise to understand what it takes to get an electron in the wire.

I am proud to stand today with my colleague Senator CAPITO and introduce a bill to roll back the EPA rule on carbon emissions—that rule which threatens the supply of abundant, affordable, and reliable electricity in North Dakota. I pledge to register my displeasure through multiple channels. This legislation today is the most public way of expressing not just my frustration but the frustration and concern of my State regulators and my State utilities.

Although this rule will have dramatic consequences across the country, it unfairly targets North Dakota utilities. During the original draft rule, North Dakota's allocation was 11 percent. This is not something we were happy with given the extent of the jurisdictional reach but something that people started rolling up their sleeves saying if we have to reduce by 11 percent, how are we going to do it and how are we going to meet this challenge? That is the North Dakota way, to not only fight for our rights but also look at what the alternatives are. Unfortunately, when the draft rule went from an 11-percent to a 45-percent reduction in the final rule, that was the straw that broke the camel's back.

I am trying to do everything I can to push back against EPA's burdensome powerplant rules to find workable solutions so North Dakotans can continue to have low-cost, reliable electricity. This CRA is one of the many different avenues I am taking to make sure that North Dakota is treated fairly.

I want to talk about what is unique about North Dakota. In fact, a lot of the generation that happens in North Dakota is generation that is generated by rural electric co-ops. These co-ops own and operate about 90 percent of the State's coal-based generation facilities, and they provide electricity to rural areas that in the past other utilities would not serve, not just rural areas in North Dakota but rural areas all through the region. These are people at the end of the line, as we call them, the very people that this rule will most impact and that EPA and this administration failed to consider when they made this final rule.

North Dakota's utilities are heavily invested in coal-based generation for a good and historic reason. I think this is an important point to make because a lot of people may say: Well, what is the difference? You can fuel switch. But at the time our electric co-ops built these generation facilities, they used coal because it was against Federal law to use natural gas. The fuel use act made it illegal to use natural gas for power generation, virtually forcing these power companies to make the investment that they made in this fuel source of coal. Now, after making billions of dollars of investments to meet the mandates under the fuel use act and to meet the numerous emissions standards that have been put forth by EPA, the administration once again is straining these assets, causing them in many cases to be stranded. If the administration were willing to pay fair market value to strand these assets, then maybe we could have a discussion, but I don't see that deal on the table. These utilities built, modified, and retrofitted all at great cost and according to Federal law at the time, and now they are threatening the very existence of this generation.

These assets are not just critical to North Dakota. Our coal-based generation provides dependable, affordable, reliable baseload electricity to millions of people in the Great Plains with roughly 55 percent of electric power generated in North Dakota being shipped outside our border.

When this final rule came out, I simply said that it was a slap in the face to our utilities and our regulators. This final rule was so vastly different from the rule that was proposed, it was almost laughable that EPA said it wasn't in any way informed by any real input or any real comment. How can you take a utility and a State from 11 percent to 45 percent and not reissue that rule? How can that be the movement in the final rule?

I think this final rule is a rule that jeopardizes close to 17,000 good-paying jobs in my State. It provides power for rural communities that otherwise would struggle for affordable, reliable baseload power. We have some of the lowest power costs in the country because we have some of the best utilities in the country, which are always looking out for the consumer at the end of the line.

North Dakota has never stepped down from a tough challenge, especially when the challenge is fair, the goal is attainable, and the timeline is achievable, but that is not this rule. The goal is not fair, the challenge is not fair, the goal is not attainable, and the timeline is unachievable in my State—unachievable. That is not anything the Clean Air Act ever anticipated—that we would set a goal with no feasible or possible way of meeting that goal, given current technology. Yet that is the position we are in.

At the end of the day, what matters most is making sure that our utilities can do their jobs, making sure that when a North Dakotan or a South Dakotan or someone from Wyoming or Colorado, where we deliver power—and certainly those in Minnesota—reaches over to turn on that light switch, regardless of the time of the day, that light comes on. That is called baseload power. People who think this is easy, people who think this is just switch fuels or switch technology, have never sat in a boardroom as I have and listened to the challenges of putting that electron on that wire.

I stand with my colleague from West Virginia and my colleague JOE MANCHIN here on our side of the aisle saying enough is enough. This is a problem we need to address. Maybe that is the difference in how we look at this. This is an issue that we can tackle and achieve results over time, but this rule is wrong. It is wrongheaded. It will, in fact, cause huge disruption to the economy of my State and the economy of the middle of this country. We have to do everything we can to prevent this rule from becoming a reality.

Thank you for letting me join you, the great Senator from West Virginia. We have two great Senators from West Virginia here.

I yield the floor.

The PRESIDING OFFICER. The majority leader.

Mr. MCCONNELL. Mr. President, there is a war on coal in America—a war on coal in America. The leader is the President of the United States. A number of us were in the Senate in 2009 and 2010, and the administration

couldn't pass their cap-and-trade proposal through the Senate. They had 60 votes in the Senate. The President and his party had 60 votes in the Senate, but they couldn't pass the cap-and-trade proposal through this body, so they decided they were going to do it anyway. They decided they were going to do it anyway.

As the two Senators from West Virginia can attest, we have a depression in central Appalachia, created not because of anything we did here in Congress but because of the President's zeal to have an impact worldwide on the issue of climate. I suspect that even if we follow this path all the way to the end, this effort by the United States would have about as much impact as dropping a pebble in the ocean. Yet we are paying a real price for it here at home. Eastern Kentucky looks like the Dust Bowl during the thirties—no jobs, no opportunity, no future, not as a result of anything we passed through the people's elected representatives but by this sort of arrogant, singlehanded messianic goal to deal with worldwide climate.

Our options to stop it are quite limited. We do have the possibility of the Congressional Review Act, but the weakness of that obviously is that even though we can pass it with a simple majority, he is likely to veto it.

We are here today to stand up for our people, the ratepayers of America, and not only the ratepayers—90 percent of the electricity in Kentucky comes from coal—but the communities that have been devastated by this. I have never seen anything like it. I heard my parents talk about what the Depression was like. It sounds and looks a lot like the stories they told me about America in the 1930s.

This is a venture that will have no impact on the issue for which it is being pursued but is having a devastating and current adverse impact on the people we represent.

We have representatives from both parties here on the floor today working toward overturning the administration's deeply regressive energy regulations. These regulations are going to ship more middle-class jobs overseas. I told my constituents last year: Coal has a future; the question is, Does coal have a future in this country? The Indians and the Chinese are not going to give up their future by not using this cheap and abundant source of power. The Germans—one of the greenest countries in Europe—are now importing coal. So coal has a future. The question is, Does it have a future here after this administration?

My folks can't even put food on the table. The ones who can find a job somewhere are leaving. The population continues to decline.

As I said earlier, it is not going to have much of an impact on the environment of our planet. This isn't going to do anything meaningful to affect global carbon levels. It just seems that someone wants to be able to pat themselves on the back for doing something even if they accomplish hardly anything at all, except hurt a whole lot of Americans. Higher energy bills and lost jobs may be trivial to some folks out on the political left—not their jobs; they don't care—but it is a different story for the middle-class Kentuckians whom I represent.

So here we have on the floor Senators from both parties who are saying it is time to take off the ideological blinders and instead think about those who have already suffered enough over the past few years. We have worked together to file bipartisan measures that would overturn the administration's two-pronged regulations. I have joined with Senator HEITKAMP and Senator CAPITO on a measure that would address one of those prongs, the one that pertains to existing energy sources. Senator MANCHIN is here on the floor and joined me as I introduced a measure that would address the other prong, the one that pertains to new sources. These bipartisan measures together represent a comprehensive solution. As I said, I am pleased to be joined here on the floor by Senators from West Virginia and North Dakota. Senator DAINES from Montana is here—another important coal State. The chairman of our Environment and Public Works Committee, Senator INHOFE, is here, and some have already spoken and some will speak after me. I am proud and pleased to be here on the floor with all of my colleagues standing up for our aggrieved constituents who have been mightily abused by this administration.

I yield the floor.

The PRESIDING OFFICER (Mr. PERDUE). The Senator from West Virginia.

Mr. MANCHIN. Mr. President, first of all, I want to thank my colleagues, Senator MCCONNELL, Senator CAPITO, who is my colleague from the State of West Virginia, Senator DAINES, Senator INHOFE, and my good friend Senator HEITKAMP.

This is a bipartisan approach. Not often do we see a bipartisan effort, a bipartisan colloquy on the floor of the Senate anymore, and there should be because we all have the same interests. Basically, how do we provide affordable, dependable, and reliable energy? That is what this country was built on. We have defended this country by having resources that we could use to basically defend ourselves, and that resource has come from what the Good Lord gave us. Coal has been in abundance in the United States of America. We have fought every war, we have defended, we have energized, and we have built a middle class unlike at any time in the history of this world.

So now it comes to the point where there is a group—basically the ones on an ideological pathway—who says we can do it differently. If someone came to me and said: We have this new great energy, and I am sorry, West Virginia and North Dakota and Oklahoma and Montana, we have this new energy—and maybe it is commercial hydrogen, which will be water vapor—that is wonderful. We will figure a way. We will embrace that. We will figure a way to make it. We will do something. We will diversify. That is not the case. The case is simply this: This country has depended and will depend—even by this administration's admission, this country will depend on fossil fuel for at least the next three decades. It is in the EIA report. They are going to have to have it. Baseload, as the Senator from North Dakota said, is simply this: something that will give us power 24/7, day and night, rain or shine. There are only two things in the world that can do it: coal and nuclear. Gas is coming on and gas will be a baseload when the distribution lines and the pipelines are there to provide it. Right now it is not, but it is coming on strong.

Just look no further than Japan. Japan was mostly moving toward nuclear. Fukushima happens. When that happened, Japan had to change. What did they do? They changed to coal. But they decided the new plants they would build would be ultra super critical. That means 40 percent efficiency, burning at the highest levels to reduce the emissions. They are moving in technology ways.

Now, what does the plan that we are talking about and we have our colleagues talking about—existing source, which means they can't continue with what we have today, and new source, which means any new plant has to be built to certain standards. Carbon capture sequestration has not been proven commercially, not at one plant in America. Yet these rules are based on using carbon capture sequestration.

All we have said—some of us have said this: Why don't you at least demonstrate that you can have that type of commercial operation and that it can withstand 1 year under commercial load and show us those are the new limits you want us to meet? That, to me, is reasonable.

Let me tell my colleagues this: If you were in the business of producing power and you desired not to do that even though we had technology, then you would have to close your plant. I understand that. That is not the case. They can't show us technology and show us that it has a commercial feasible pathway to be able to perform and provide the energy we need. There is no way they can do it.

So I have said this: If it is unobtainable, it is unreasonable. That is all. Don't expect me to do something that has never been done. If the Federal Government says: Fine, we have $8 billion lying down at the Department of Energy—$8 billion that hasn't been tapped—does that not tell us something?

The private sector has not stepped up to take those types of loans and to use those types of loans to find the new technology for the future because they don't believe the administration wants

us to find any new technology that might be able to adhere to the standards they have set.

So we sat back and we have done nothing. Then, on top of that, they expect these plants, 30 years from now—if they are expecting to get commercial power, electricity, fill the grid with power coming from coal for the next 30 years—most of our plants average 50 years of age. They can't produce the power they are going to produce—that we will need for this country to have for 30 more years. An 80-year-old plant just won't do it. So that means they come off the line, off the grid. When that comes off the grid, what we call dependable, reliable, and affordable energy goes away. It goes away.

I have said this: Someone needs to respectfully ask our President, this administration, the EPA, the DOE: If for the next 90 days not another ton of coal was delivered to a coal plant in America—not another ton of coal because—and I have said this to the administration. They have been very eloquent in basically telling the American people: We don't like coal, we don't want coal, and we don't need coal. If those were the facts, then make sure you tell the American people, if they didn't have coal for 90 days, what the United States of America would look like. Just tell me what it would look like. Ask anybody what it would look like. The lives of 130 million people would be in jeopardy tomorrow—130 million people. This system could collapse. The east coast could be dark. Now, you tell me how you are going to fill that in. And if you are not willing to be honest with the American people and tell them that, don't make them believe there is something that is not there, that you can run this off of wind and solar.

We have a lot of wind in West Virginia, and we are proud of that. I will give an example. My colleagues will remember the hottest days this past summer, that very hot spell we had, 90 to 100 degrees. We have 17 acres of a wind farm on top of a beautiful mountain in West Virginia, 560 megawatts. We have a coal-fired plant sitting there, the cleanest super-critical coal-fired plant on Mount Storm, 1,600 megawatts. Guess how many megawatts of power the wind produced during the hottest times of the summer when we needed the power. Two megawatts. Two. The wind didn't blow. It was so hot and stagnant, it didn't blow. That poor little coal-fired plant was giving it everything it had to try to produce the power the Nation needed.

I am just saying the facts are the facts whether we like them or not. So when this plan comes out and says that any new coal-fired plant being built has to be—you can basically be assured they are not going to build any. When they are saying existing plants have to meet certain standards, they won't invest and try to hit a moving target.

So now what happens? For the 35 to 40 percent of the power you are telling the United States of America, the people in this great country, that we have—don't worry, we are going to take care of you, it is not going to happen. We are not going to stand by and say we are not going to fight for that. We are not only fighting for a way of life for West Virginia, we are fighting for a way of life for this country.

This country depends on energy we have been able to produce. We have always depended on our little State. North Dakota, now one of the best energy-producing States we have in the country—Montana, Wyoming, Oklahoma—we have been the heavy lifters. We will continue to work for this great country. We just need a little help. That is all we are asking for.

So I would say, ask the question: What would the country look like tomorrow? The standards they are setting are basically unreasonable, totally unreasonable, because they are unobtainable.

The impact is going to be devastating, basically. The system is going to be to the point to where we can't depend on it, it is not reliable, and we don't have the power of the future yet. Maybe our children or grandchildren might see that. I hope so. But until the time comes where we are going to transition from one to the other, make sure it is a smooth transition. Make sure it is a dependable transition. Make sure it is one that keeps this country the superpower of the world. If we don't, I guarantee we will be the last generation standing as a superpower saying that we are energy independent; we are not fighting wars around the world basically for the energy this country needs. We have the ability to basically take care of ourselves. We can be totally independent with energy if we have an energy policy that works, but it has to be realistic. This is not.

That is why I totally oppose this new power plan which is coming out. It is a shame that we have to rely on the courts to protect something we should be doing in the Halls of this Senate. It is a shame that the courts have to step in to protect us.

With that being said, I yield the floor, and I thank my colleagues for being here on this important issue.

The PRESIDING OFFICER. The Senator from Oklahoma.

Mr. INHOFE. Mr. President, first of all, I appreciate the fact that my colleagues from West Virginia, North Dakota, Kentucky, and Montana—all of us are getting together on this in a bipartisan way. I think it is worth repeating, to make sure everyone understands where we are on this, what a CRA is. The CRA is the Congressional Review Act. It is an act that allows an elected person who is answerable to the public to weigh in on these decisions that are made by the President—who can't run again for office—and by the unelected bureaucrats who are destroying this country.

As was pointed out by the Senator from Kentucky, I do chair the committee called the Environment and Public Works Committee. On this committee, we deal with these regulations. We have jurisdiction over the EPA. It is interesting I would say that because we tried to get the EPA to come in and testify as witnesses as to how the President plans to move to the percentage of power that is going to be generated by the year 2030 by renewables, and they won't testify because they don't have a plan. They don't know how they are going to do it.

The CRA is significant because there are a lot of people in this case who would be the liberals in this body who like the idea of being overregulated, who like the idea of having the regulators run our lives, and they are the ones who would love to go home when people are complaining about the cost of all of these things and they can say: Well, wait a minute. Don't blame us. That was a bureaucrat who did that; that wasn't me.

Well, this forces accountability, and these guys don't like it. I can assure you right now that we are going to give everyone an opportunity to weigh in on what these issues are. They would much prefer to go home and say: I know we are overregulating and I know it is destroying the States—whatever the States happen to be—but it wasn't me, don't look at me.

Now we are going to see who is responsible because what is going to happen is we are going to have a vote. The vote is going to take place, and I think our leader is correct when he says the President will probably veto this. If the President vetoes it, it comes back for a veto override, and then people will know who is for it and who is against it. So I think a CRA has another great value. It forces accountability by people who are answerable to the public.

On the issue we are discussing today, the interesting and the consistent pattern we have is that what this President does is he gets the things they tried to do through over—through legislation, and those things that fail through legislation he tries then to do by regulation.

Let me give you an example. Another issue—not the issue we are talking about today—is the WOTUS issue, the waters of the United States. Historically, it has been the States that have regulations over the waters except for navigable waters. Well, of course, liberals want everything in Washington. So 5 years ago a bill was introduced, and the bill would have essentially taken the word ''navigable'' out so that the Federal Government would have control over all the waters in my State of Oklahoma and throughout America. Two of them introduced a bill, one was Senator Feingold of Wisconsin and the House Member was Congressman Oberstar from one of the Northern States. I don't know which one it was. They introduced a bill to take the word ''navigable'' out. Not only did we overwhelmingly defeat the legislation, but the public defeated the two of them in the next election.

Now the President is trying to do what he was not able to do through legislation through regulation. The same thing is true—the Senator from West Virginia is right when he talked about what they are trying to do. It is very interesting when you look at this bill. We are talking about the emissions of CO_2. The first bill that was introduced was in 2002. It was the McCain-Lieberman bill. We defeated that. The next one was the McCain-Lieberman bill in 2005, and the third one was the Warren-Lieberman bill in 2008. Then we had the Waxman-Markey bill that we never even got to vote on because nobody was going to vote for it.

So what they fail to be able to do legislatively, they are now trying to do through regulations, and that is why a CRA is significant because it does force accountability.

Let me make one other statement. This thing about Paris that is going to take place in December. This is the big party that the United Nations puts on every year. It is the 21st year they have done this. I can remember when they did it in 2009. That was going to be Copenhagen. Several people went over there at that time. President Obama was in the Senate, Hillary was in the Senate, PELOSI was there, and John Kerry went. They went over there to tell the 192 countries that were meeting in Copenhagen—the same 192 countries that will be meeting in 2 months—went over to tell them we were going to pass cap-and-trade legislation that year. That was 2009.

I went over after they had given their testimony there. I went all the way over to Copenhagen, spent 3 hours, and came all the way back on the next flight. I probably had the most enjoyable 3 hours I ever had because I was able to talk to 192 countries and tell them they had been lied to; that we are not going to be passing it. The same thing is going on in December of this year.

By the way, let me just mention one thing that hasn't been said. There are people out there listening to this who actually believe this stuff, that the world is going to come to an end because of CO_2 manmade gases. This is something we have been listening to for a long period of time. I remember right before going to Copenhagen in 2009—at that time the Administrator of the Environmental Protection Agency was Lisa Jackson, an appointee by President Obama, and I asked her this question on the record, live on TV. I asked: If we had passed any of the legislation or the regulations that we are talking about passing, would this have an effect of lowering the CO_2 worldwide? She said—now keep in mind this was an Obama appointee—by the way, Obama was President at that time when he went to Copenhagen. She said: Well, no, it wouldn't reduce emissions worldwide because it just pertains to the United States.

This isn't where the problem is. The problem is in India, it is in China, it is in Mexico. The problem we would have there is, yes, we might lower our CO_2 emissions in the United States. However, those other countries will not, and it could have the effect of increasing, not decreasing, CO_2 emissions because as we chase our manufacturing base overseas to places they don't have any restrictions, we would have the effect of increasing it.

So I am just saying I appreciate the fact we are all together on this and making the necessary efforts to make people accountable. I think it might surprise a lot of people as to who changes their mind on this once they know they have to cast a vote and be accountable.

I applaud, certainly, my friends from West Virginia and the other States that are involved in this. I think this is the right thing to do. Let's keep in mind the Utility MACT—that is the maximum achievable control technology—was the first shock to put coal under. At that time we did a CRA, and we actually came within four votes of getting the bill passed, and that was when Republicans were not a majority. I look for some good things to happen, and I think we are doing what is right and responsible.

I yield the floor.

The PRESIDING OFFICER. The Senator from West Virginia.

Mrs. CAPITO. Mr. President, I ask unanimous consent for additional time so the Senator from Montana can join the colloquy. As he reminds me, the Senator has the largest recoverable tonnage of coal in the Nation.

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

Mr. DAINES. Thank you, Mr. President.

This administration is shutting down coal-fired powerplants in the United States. I thank the Senator from West Virginia, Mrs. CAPITO, the other Senator from West Virginia, Mr. MANCHIN, and we have Senator HEITKAMP here. We had Democrats and Republicans in colloquy talking about what is going on with coal-fired plants and the Clean Power Plan of this administration.

This is what is happening. It is killing good-paying jobs for union workers, for pipefitters, for boilermakers, and tribal members in my State with these so-called Clean Power Plan regulations. At the same time, it is stifling investment that could lead to innovation to make coal cleaner in the United States.

As I travel across Montana, I have heard Montanans describe the EPA as—a rancher once told me it stands for ''Eliminate Production Agriculture.'' A union member recently told me it stands for the ''Employment Prevention Agency.'' President Obama and his ''Employment Prevention Agency'' continues to wage war on American energy, American families, and on American jobs. This so-called Clean Power Plan is an all-out frontal assault on affordable energy and good-paying union jobs as well as tribal jobs. This will leave President Obama directly responsible for skyrocketing energy bills, a loss of tax revenue for our schools, teachers and our roads and the unemployment of thousands of hard-working Americans. The President ignores the fact that more than half of Montana's electricity comes from coal, as do thousands of jobs and $120 million in tax revenue every year.

In fact, 40 percent of our Nation's energy comes from coal. When a young person plugs their iPhone or their smartphone into the wall and charges it, most likely it is being charged by coal.

In my hometown of Bozeman, we have a Tesla charging station at one of our hotels. Elon Musk at Tesla did an amazing, innovative job creating electric vehicles, but when they plug those Tesla vehicles into those chargers, those Tesla vehicles in Montana are likely powered by coal.

The facts are that coal production in the United States is much safer and less carbon intensive than coal from other nations. As had been mentioned, this is a global challenge we must think about and address. The Powder River Basin in Southeast Montana has coal that is among the cleanest in the world. It has lower sulfur content and cleaner than Indonesian coal. Shutting down U.S. coal will have a negligible impact on global coal demand and global emissions. However, it will ultimately make it more likely that less technologically advanced coal production techniques will be used around the world.

This is the way to think about it. The United States consumes about 10 percent of the world's coal. Said another way, 90 percent of the coal consumption in the world occurs outside the United States, and the global demand for coal-fired energy will not disappear even if the United States were to shut down every last coal mine and every last coal-fired plant.

Again, individuals are entitled to their own opinions but not to their own facts. Here are the facts. Coal use around the world has grown about four times faster than renewables. There are 1,200 coal plants planned across 59 countries. About three-quarters of them will be in China and India. China consumes 4 billion tons of coal per year versus the United States at 1 billion tons. China is building a new coal-fired plant every 10 days, and that is projected to last for the next 10 years.

In Japan—I used to have an office in Tokyo. My degree was in chemical engineering, and I was part of a software company with offices around the world. I remember the big earthquake that struck Japan—the 9.0 quake. The Fukushima nuclear reactors were disabled. How is Japan dealing with that? They are building 43 coal-fired powerplants. By 2020, India may outbuild 2½ times more coal capacity as the United States is about to use. So it is shortsighted and misguided to move forward on an agenda that is going to devastate

significant parts of the economy. It is going to raise energy prices and destroy union jobs and tribal jobs.

We are seeing that already in Montana. Earlier this month, in the month of October, a customer of the Crow Tribe, the Sherco Coal plant in Minnesota announced it needs to shut down two units. This cuts off a significant portion of the customer base for Crow coal. Because the Crow Tribe relies on coal-fired Midwest utilities for most of its non-Federal revenue and for good-paying private jobs at the Absaloka Mine, the unemployment rate on the Crow reservation today is in the high 40 percent. Without these coal mining jobs, that unemployment rate will go to 80 to 85 percent.

Ironically, some of the first impacted by the Obama administration's new regulations are those who can least afford it. You have heard it from Senators on both sides of the aisle today. Under the final rule, the Colstrip powerplant in Montana will likely be shuttered, putting thousands of jobs at risk. We must take action. We need to stop these senseless rules.

This past weekend I joined the Montana attorney general, Tim Fox, in Helena to announce that Montana, along with 23 other States, has filed a lawsuit against the Federal Government because of Obama's recent decision. There are currently 26 States—the majority of the States in this United States—through three different lawsuits that have requested an initial stay on the rule.

As Leader MCCONNELL mentioned in 2010, a Democratic-controlled Congress could not pass these regulations. The people's House stopped it, but now President Obama and the EPA are moving forward without the people's consent.

I am thankful to partner with a bipartisan group of my colleagues, Leader MCCONNELL, Senator CAPITO, Senator INHOFE, Senator MANCHIN, and Senator HEITKAMP, who are speaking out and working to stop this harmful rule. I am proud to stand and join them as a cosponsor of two bipartisan resolutions of disapproval under the Congressional Review Act that would stop the EPA from imposing the anti-coal regulation.

Coal keeps the lights on, it charges our iPhones, and it will continue to power the world for decades to come. Rather than dismissing this reality, the United States should be on the cutting edge of technological advancements in energy development. We should be leading the way in using clean, affordable American energy.

America can and should power the world. We can only do it if the Obama administration steps back from the out-of-touch regulations and allows American innovation to thrive once again. In summary, we need more innovation, not more regulations.

Thank you, and I yield back my time.

The PRESIDING OFFICER. The Senator from West Virginia.

Mrs. CAPITO. Mr. President, I would like to thank my colleagues for joining me in a colloquy, particularly the Senator from North Dakota, who is cosponsoring the Congressional Review Act legislation with me on existing coal-fired powerplants, and certainly my colleague from West Virginia Senator MANCHIN. We have worked very well together in a bipartisan way on these issues—Leader MCCONNELL, Chairman INHOFE, and Senator DAINES from Montana.

I think we have presented a clear picture of the impact of these rules. So I ask unanimous consent that any time spent in a quorum call before the 4 p.m. vote series be charged equally against both sides.

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

Mrs. CAPITO. I yield the floor.

The PRESIDING OFFICER. The Senator from Florida.

PUERTO RICO

Mr. NELSON. Mr. President, I want to talk about the financial crisis that is going on in Puerto Rico. We have all heard about the current situation that Puerto Rico finds itself in. They are suffering. They are having trouble paying their bills and their economy is in shambles. Some people have the attitude ''Well, that is not our problem,'' but they are forgetting the fact that Puerto Rico is part of the United States. It is a territory. It is not a foreign country. Puerto Ricans are American citizens.

If a problem exists in Puerto Rico, it exists in the United States. It is not something we can just ignore. It impacts the entire country. If the economy continues to suffer in Puerto Rico, the people there will just move to another part of the country. I want to repeat that. If things are bad in Puerto Rico economically, they—Puerto Ricans—can move to another part of the country. This is not immigration; this is a move to the mainland. Many Puerto Ricans are leaving Puerto Rico because of it is troubles.

Happily, many of the people who live on the island are moving to Florida. They are adding to the diversity and immense fabric of Florida that reflects the entire country, but our gain in Florida is Puerto Rico's loss. There are more than 1 million people in Florida alone who may have preferred to stay at home on the island with their friends and their families. People who otherwise would be opening small businesses or new doctors' offices in San Juan are opening them in Orlando. This only hurts Puerto Rico's economic future.

We need to give Puerto Rico the tools it needs to get its economy back on track. Puerto Rico cannot do that alone. Congress needs to pitch in. I have joined a number of our colleagues—BLUMENTHAL, SCHUMER, and MENENDEZ—in being a sponsor of the Puerto Rico Chapter 9 Uniformity Act. It fixes a glitch in the Federal bankruptcy law that stops Puerto Rico's municipalities and public corporations from restructuring their debt through the Federal bankruptcy court, something that is law in all of the States. That is why we have a bankruptcy law, but there is a glitch that you cannot do that in Puerto Rico. That is simply unfair. The people of Puerto Rico should get equal protection under the law.

Both the Finance Committee and the Energy and Natural Resources Committee have held hearings in the past few weeks about the economic crisis in Puerto Rico. Two of Puerto Rico's elected officials, Governor Garcia Padilla and Congressman PIERLUISI, have testified at these hearings. Both said that Puerto Rican public corporations need access to Chapter 9 debt restructuring.

It is this Senator's strong desire that we see them treated equally under the law and that this legislation to fix this glitch comes to the floor soon. We also need to help Puerto Rico's health care system. The Medicaid Program in Puerto Rico serves nearly 1.7 million residents. It is in terrible shape. In 2010, Congress passed the Affordable Care Act, which provided Puerto Rico with a $5.4 billion one-time payment to cover health care costs. That money is set to expire in 2019, but it could even run out sooner.

Under Medicare Part D, Puerto Rican residents are being treated like second-class citizens. They don't get the same financial support that State residents get for prescription drug coverage. This has an effect on their economy, stifling their ability to emerge from the crisis, not to speak of the fact that they are not getting the health care other American citizens have.

I remind you, Puerto Ricans are American citizens. So this kind of treatment under Medicare flies in the face of the most basic American value—equality. That is why several of us have joined Senator SCHUMER on a bill to improve the way Puerto Rico is treated under Medicare and Medicaid.

Last week, thankfully, the White House released a set of legislative proposals to help Puerto Rico. Included in that list were some of the bills I have mentioned here that I support. I urge our colleagues to give this problem the attention it demands. We should move the proposals that we can move in this legislative body. We should do it with haste. There are more than 3½ million people in Puerto Rico. They are U.S. citizens who, unlike most U.S. citizens, have no one to represent them in this Chamber and only have a nonvoting delegate in the House of Representatives. They have no voice here, but even with no voice, there are some of us in this Chamber who will make sure that their voice is heard. We cannot turn our backs on fellow Americans. By the way, when it comes time to defend this country and our national security, look at the percentage of Puerto Ricans who sign up for the military. They are fellow Americans. I ask my colleagues to look deep in their hearts

and find a way to come together to help the island of Puerto Rico, a territory, our fellow American citizens, to get through this troubled time.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

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

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

BUDGET AGREEMENT

Mr. NELSON. Mr. President, since I see no one is waiting to speak, I might offer a couple of comments about the proposed budget agreement. We are still evaluating this, looking at the details, but first things first. This seems to me to be something we should agree to. It certainly gets us past this artificial debt crisis that would cause the United States to go into economic cataclysmic fits.

If we do not raise the debt ceiling, America cannot pay its obligations it has already incurred. It would be the first time the U.S. Government went into default. That time has already run out, but through extraordinary measures the Secretary of the Treasury has been able to keep the cashflow going, but he is running out of all of his tricks of the trade next week, November 3. That is the first thing it would do most immediately.

The second thing it would do is it would get us over this budgetary impasse of a budget that lays out the blueprint—for the flushing out of that blueprint, which are the appropriations bills. So in the case of the budget, what had been brought forth was a budgetary gimmick of saying we were going to raise the amount of money we needed for defense, but it was not going to meet this arbitrary budget cap that had been set 3 years ago by the cuts across the board called the sequester. But oh, by the way, we were going to increase that defense spending a little more by creating an additional account over and above what we spend overseas called the overseas contingency fund, OCO, and therefore money was going to be supplied—the increases we need in defense—with in fact not increasing the budgetary caps on spending.

Well, that was budgetary fakery. That was budgetary sleight of hand. That was not budgetary truth. This agreement stops that for the next 2 years. Two years from now we will have to face the same thing and get rid of this artificial cut across the board. That is no way of dealing with trying to cut the budget. You ought to be cutting the budget with a scalpel, not with a meat cleaver, where you come across the board on every program.

Indeed, what this agreement does is it raises the caps on defense in this first year $25 billion. It allows an OCO increase of $23 billion—and that is considerably less than what had been proposed earlier. Indeed, as you get into fiscal year 2017, it raises the budgetary caps on defense by $15 billion, also a $23 billion OCO, or overseas contingency fund, for the war effort over in Central Asia.

This is a good program, but the other thing this agreement corrects—in the Republican budget, they had only raised money for defense spending, and all the other needs of government that need to be appropriated—nondefense discretionary spending—were kept artificially low. If you are talking about grants from NIH, that was all being limited. If you are talking about money for NASA as we get into the program of going to Mars, all of that had been cut. If you are talking about agricultural programs, all of that had been cut. No matter what program—education, the environment, you go on down the list—all of that had been cut.

This budget agreement that we will vote on hopefully in the next 2 or 3 days does, in fact, raise those budgetary caps for nondefense spending as well as for defense spending. So where the caps were raised in this first year of fiscal year 2016 by $25 billion for defense spending, so too $25 billion for nondefense discretionary spending. Likewise, in the next fiscal year, 2017, where the caps had been raised $15 billion for defense spending, likewise, nondefense discretionary and all those other needs of government, the same amount—$15 billion.

I will have more to say about this later, but while I have the opportunity, I wish to commend to the Senate that I think it is certainly in the interests off of our country to move forward and approve this new budgetary agreement.

By the way, I might add as I close that an agreement has been hammered out between the Republican and the Democratic leadership in both Houses, along with the White House.

I yield the floor.

Mr. LEAHY. Mr. President, in today's digital age, many Americans live their lives online. We communicate via email, use photo sharing and social networking Web sites, store documents in the cloud, and access our private financial and medical information through the Internet. The amount of sensitive electronic data that we create and store on the Internet is staggering and will only continue to grow. We know that cyber security is an important component of protecting our critical infrastructure. A cyber attack targeting the electric grid in the Northeast, for example, could have dire effects during a cold Vermont winter. I know that Vermonters care about cyber security, and Congress must act responsibly to strengthen our ability to defend against cyber attacks and breaches. But I also know that Vermonters care deeply about their privacy and civil liberties, and I believe just as strongly that whatever Congress does in the name of cyber security must not inadvertently undermine the privacy and security of Vermonters and all Americans.

For years, Congress has seemed singularly focused on the private sector's desire for voluntary information sharing legislation. While improving the flow of cyber threat information between the government and private sector is a laudable goal that I support, it is not a panacea for our cyber security problems. Information sharing alone would not have prevented the major breaches of the past year, such as the breach at the Office of Personnel Management, OPM, or the breaches at Sony, Home Depot, or Anthem.

Narrowly tailored legislation to facilitate the sharing of technical, cyber threat data could be beneficial, but the Senate Intelligence Committee's bill lacks certain basic safeguards and threatens to significantly harm Americans' privacy. That is why I have heard from a number of Vermonters who oppose the bill and that is why consumer advocacy organizations, privacy and civil liberties groups, and major technology companies like Apple, Dropbox, and Twitter all vocally oppose the bill. The technology companies know firsthand the importance of ensuring our cyber security, and they oppose this bill because they believe it does little to improve our cyber security and would ultimately undermine their users' privacy.

For months, I have worked with Senator FEINSTEIN to improve this bill. She has been receptive to my concerns, and I appreciate that many of the revisions that I suggested are now incorporated into the managers' amendment. The managers' amendment now makes clear that companies can only share information for cyber security purposes, which is an improvement from the original legislation. It also prohibits the government from using information shared by private companies to investigate routine crimes that have nothing to do with cyber security. And it removes a completely unnecessary and destructive new exemption to the Freedom of Information Act, FOIA, which had the potential to greatly restrict government transparency. These are significant improvements, and I am thankful to Senator FEINSTEIN for working with me to incorporate them into the bill.

Unfortunately, the Senate Intelligence Committee's bill still has major flaws. This bill overrides all existing legal restrictions to allow an unprecedented amount of data—including Americans' personal information—to flow to the government without adequate controls and restrictions. It needlessly requires all information shared with the government to be immediately disseminated to a host of Federal agencies, including to the NSA. It fails to adequately require companies to remove irrelevant personal information before sharing with the government. The bill contains broad authorizations that allow companies to monitor traffic on their networks with liability protection and employ ''defensive measures'' that may

cause collateral harm to innocent Internet users. The bill also continues to include another unnecessary FOIA exemption that will weaken the existing FOIA framework.

Proponents of the bill have attempted to assuage many of these concerns by arguing that sharing under this bill is voluntary, and if companies do not want to share information with the government or use the authorities in the bill, they do not have to. This bill may be voluntary for companies, but it is not voluntary for consumers. American consumers have no say on whether their information is shared with the government and ends up in an NSA or IRS database. They may have no recourse if a company needlessly monitors their Internet activity or inappropriately shares their personal information with the government.

Rather than limiting the dissemination of information in order to protect the private and proprietary information of Americans and American businesses, this bill goes in the wrong direction by giving companies more liability protection and more leeway on how to share our information. The most effective action Congress can take to improve our cyber security is to pass legislation that requires companies to take greater care of how they use and protect our data, not less. And we should pass my Consumer Privacy Protection Act to require companies to protect our personal information and help prevent breaches in the first place. The cyber security legislation before us today does nothing to address this very real concern, so I cannot support it. I fear that this bill will significantly undermine our privacy, and I urge Senators to vote against passage.

The PRESIDING OFFICER. The Senator from Arkansas.

Mr. COTTON. Mr. President, I ask unanimous consent to speak for up to 15 minutes.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

AMENDMENT NO. 2581, AS MODIFIED

Mr. COTTON. Mr. President, today I speak in support of the Cotton amendment to the Cybersecurity Information Sharing Act. My amendment is straightforward. It simply would provide liability protection to any business or other private organization that shares cyber threat indicators to the FBI or the Secret Service.

In its current form, the Cybersecurity Information Sharing Act would require entities to submit these cyber threat indicators through a portal created and run by the Department of Homeland Security in order to receive liability protection. But there are also two exceptions that would allow entities to receive liability protection outside the DHS portal: first, if a submission was related to a previously shared cyber threat indicator, and second, if the submitting entity is sharing information with its Federal regulatory authority. But not every private entity has a Federal regulatory authority, thank goodness, so where a cable company can share with the FCC or an energy company can go to the Department of Energy or FERC, other businesses are forced to go to the DHS portal. Good examples are retailers such as JCPenney, Walmart, Target, and Home Depot.

When the trade associations for two victims of the biggest cyber attacks in recent memory—Target and Home Depot—are pleading for this language, we should take notice and incorporate it. Anything else would be unfair, inequitable, and unwise.

We ought to give these companies an alternative to the DHS portal. One simple reason is that nobody knows what the portal will look like, how it will function, or how much it will cost companies to interact with it. The Federal Government, after all, doesn't have the best track record for designing and deploying IT systems. Healthcare.gov was not exactly a resounding success. One could easily imagine a company trying to share a cyber threat indicator and getting an error message from the portal, just as millions of Americans received when they tried to sign up for ObamaCare.

In this case, regulated businesses can just go to their regulator. Private and small businesses will be out of luck, though. This is the primary reason my amendment has such strong private support. Organizations such as the National Retail Federation, the chamber of commerce, the National Cable & Telecommunications Association, and many others support this commonsense amendment.

The second main reason that entities should be able to share directly with the FBI and the Secret Service is that the bill is about promoting collaboration between the government and the private sector, as the National Security Council says that we should in this tweet: ''More than any other national security topic, effective cybersecurity requires the US gov't & private sector to work together.'' I agree.

As Director Comey recently told the Senate Intelligence Committee, the FBI has redoubled its efforts to reach out to private businesses in this area. This has paid dividends. And there is no entity in the Federal Government that the private sector trusts more on cyber security than the FBI. That is why Sony Pictures called the FBI when it was hacked by North Koreans last year.

I also have to imagine that is the main reason the White House endorsed my amendment over the weekend when they sent out this very helpful tweet: ''If you are a victim of a major cyber incident, a call to @FBI, @SecretService, or @DHSgov is a call to all.'' My goodness, Susan Rice and I stand together in agreement that if you are a victim of a cyber incident, you should be able to call the FBI, the Secret Service, or the DHS. I thank the National Security Advisor and the White House for their support for the concept behind my amendment.

I would also like to take a few moments to dispel a few myths about this amendment. The first myth is that the Cybersecurity Information Sharing Act creates a single portal at DHS for liability-protected information sharing with the Federal Government and that the Cotton amendment would create an unprecedented second channel.

This is false. The bill authorizes multiple liability-protected sharing channels with the Federal Government, not just one, through a broad exception to the DHS portal that permits certain regulated businesses to engage in liability-protected sharing of cyber threat information directly with any Federal regulators without requiring that it first pass through DHS. The Cotton amendment simply provides the same flexibility for businesses that already have established threat-sharing relationships with the FBI or the Secret Service to maintain their existing channels for sharing and not incur significant costs and delays to establish new ones with DHS. My amendment is consistent with this multichannel sharing approach.

The second myth is that my amendment would harm privacy as it would allow the sharing of cyber threat indicators with the FBI and the Secret Service and that the sharing with these agencies wouldn't happen under the bill in its current form.

This is also false. Under the current version of the bill, if an entity shares information through the DHS portal, the FBI and Secret Service will receive it. My amendment doesn't change that or the privacy protections in the bill. Both with and without my amendment, the FBI and Secret Service will get cyber threat indicators.

The third myth is that the scrub DHS would have to conduct for personally identifiable information is not as rigorous under my amendment.

Again, this is not true. The Cybersecurity Information Sharing Act requires all Federal entities receiving threat indicators to protect privacy by removing personal information that may still be contained in them before sharing with other entities. My amendment does not eliminate or weaken any of the bill's privacy requirements, as the FBI and Secret Service are required to protect privacy in the same way all other Federal entities receiving threat indicators.

Finally, I simply want to note that the House-passed version of the bill contains a nearly identical provision, and that bill passed with overwhelming bipartisan support on a 307-to-116 vote.

To sum up, the Cotton amendment has overwhelming support in the private sector, including companies that have been victims of cyber crimes. It would lead to greater information sharing between the private sector and the Federal Government. It preserves the privacy protections in the bill. When it was included in the House bill, both

Republicans and Democrats voted yes. I therefore ask my colleagues on both sides of the aisle to support this amendment.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

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

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

Mr. BURR. Mr. President, what is the order of business?

AMENDMENT NO. 2552, AS FURTHER MODIFIED

The PRESIDING OFFICER. Under the previous order, the question occurs on amendment No. 2552, as further modified, offered by the Senator from Delaware, Mr. COONS.

The Senator from California.

Mrs. FEINSTEIN. Mr. President, I wish to speak and urge a ''no'' vote on amendment No. 2552, known as the Coons amendment.

This amendment essentially adds another layer of review to the bill's current requirements. We worked this out in an earlier amendment with Senator CARPER. This amendment goes further, and it could prevent parts of the government from quickly learning about cyber threats at machine speed because it would require an additional privacy review for any information going through the DHS portal.

The Carper amendment that I spoke about was adopted as part of the managers' package, which made clear that the government should take automated steps to ensure that the real-time information sharing system can both protect privacy and allow for sharing at the speed necessary to stop cyber threats. Because the Coons amendment will slow down sharing via the DHS portal, I ask my colleagues to join me in voting no.

The PRESIDING OFFICER. The Senator from Delaware.

Mr. COONS. Mr. President, I rise today to urge my colleagues to support my amendment to make sure that this bill strikes the right balance between privacy and security.

I respect the very hard work of Senators BURR and FEINSTEIN and the constructive amendment that my senior Senator TOM CARPER added to the managers' amendment. I do believe this bill has made significant movement in the right direction. But I remain concerned, and my amendment's purpose is to require that DHS review all cyber threat indicators it receives and to remove personally identifying information by the most efficient means practicable. It would not necessarily—according to the amendment in the managers' package—be required that DHS scrub, unless multiple agency heads unanimously agree on the scrubbing process. My amendment's purpose is to simply ensure that these privacy scrubs—done at machine speed, done in a responsible way—protect citizen privacy and our security. I don't think we should be forced to choose between those two.

I urge my colleagues to support my amendment.

The PRESIDING OFFICER. The question occurs on agreeing to amendment No. 2552, as further modified.

Mr. BURR. 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 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 (Ms. AYOTTE). Are there any other Senators in the Chamber desiring to vote?

The result was announced—yeas 41, nays 54, as follows:

[Rollcall Vote No. 289 Leg.]

YEAS—41

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

NAYS—54

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

NOT VOTING—5

Cruz	Paul	Vitter
Graham	Rubio	

The amendment (No. 2552), as further modified, was rejected.

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Madam President, I ask unanimous consent that the cloture motion on S. 754 be withdrawn; that prior to the vote on adoption of the Burr-Feinstein substitute amendment, the managers' amendment at the desk be agreed to; and that following adoption of the substitute, the bill be read a third time and the Senate vote on passage of the bill, as under the previous order. I further ask that notwithstanding adoption, the Flake amendment No. 2582 be modified with the technical change at the desk.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

The amendment (No. 2582), as further modified, is as follows:

At the end, add the following:

SEC. 408. 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. 2581, AS MODIFIED

The PRESIDING OFFICER. Under the previous order, the question occurs on amendment No. 2581, as modified, offered by the Senator from Arkansas, Mr. COTTON.

The Senator from Arkansas.

Mr. COTTON. Madam President, I support this important bill, but I want to strengthen it.

Under the bill, a business receives liability protection by reporting threats to DHS or its regulatory agency, but many businesses, especially retailers like Target or Home Depot, don't have a regulator; thus, they must report to DHS. They have no choice. They must report to DHS even if they have longstanding ties to the FBI, as did Sony Pictures.

I contend that we should allow these businesses to choose between the DHS, FBI, and Secret Service. Fortunately, the White House appears to agree with my position. The National Security Council tweeted over the weekend: ''If you are a victim of a major cyber incident, a call to @FBI, @SecretService, or @DHSgov is a call to all.''

This amendment wouldn't undermine the single-point-of-reporting concept behind this bill because there is already an exception for the regulators, nor would it impair privacy rights because those rules apply to the FBI.

Finally, I would note that the House-passed version of this bill includes a nearly identical provision, and that got 307 votes.

Let's join together in a bipartisan fashion, adopt this amendment, and strengthen the bill.

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Madam President, we are almost at the end. This is the last amendment.

Unfortunately, I rise to ask my colleagues to vote against the amendment of not only my colleague but a member of the Intelligence Committee. This is a deal-killer. I will be very honest. This kills the deal. One of the thresholds that we had to reach was the balance to have one portal that the information goes through. This creates a new

portal. The White House is not in favor of it. Downtown is not in favor of it because they understand what it does.

We are this close right now to a voluntary information sharing bill. I can assure you that this is the first step. We have a ways to go. But if you want to stop it dead in its tracks, support this amendment. If, in fact, you want to get this across the goal line, then I would ask you to defeat the Cotton amendment and let us move to passage of this bill. Let us go to conference with the House.

I yield the floor.

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

Mr. BURR. 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 senior assistant legislative 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 22, nays 73, as follows:

[Rollcall Vote No. 290 Leg.]

YEAS—22

Boozman	Kirk	Scott
Capito	Lankford	Sessions
Cornyn	McCain	Shelby
Cotton	McConnell	Thune
Fischer	Perdue	Toomey
Grassley	Portman	Whitehouse
Inhofe	Rounds	
Isakson	Sasse	

NAYS—73

Alexander	Enzi	Moran
Ayotte	Ernst	Murkowski
Baldwin	Feinstein	Murphy
Barrasso	Flake	Murray
Bennet	Franken	Nelson
Blumenthal	Gardner	Peters
Blunt	Gillibrand	Reed
Booker	Hatch	Reid
Boxer	Heinrich	Risch
Brown	Heitkamp	Roberts
Burr	Heller	Sanders
Cantwell	Hirono	Schatz
Cardin	Hoeven	Schumer
Carper	Johnson	Shaheen
Casey	Kaine	Stabenow
Cassidy	King	Sullivan
Coats	Klobuchar	Tester
Cochran	Leahy	Tillis
Collins	Lee	Udall
Coons	Manchin	Warner
Corker	Markey	Warren
Crapo	McCaskill	Wicker
Daines	Menendez	Wyden
Donnelly	Merkley	
Durbin	Mikulski	

NOT VOTING—5

Cruz	Paul	Vitter
Graham	Rubio	

The amendment (No. 2581), as modified, was rejected.

Mr. COTTON. I yield back all time.

AMENDMENT NO. 2749 TO AMENDMENT NO. 2716

(Purpose: To improve the substitute amendment)

The PRESIDING OFFICER. Under the previous order, the managers' amendment, No. 2749, is agreed to.

The amendment is printed in today's RECORD under ''Text of Amendments.''

VOTE ON AMENDMENT NO. 2716, AS AMENDED

The PRESIDING OFFICER. The question is on agreeing to the substitute amendment No. 2716, as amended.

The amendment (No. 2716), as amended, was agreed to.

The bill was ordered to be engrossed for a third reading and was read the third time.

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Madam President, I ask my colleagues for just the next 2 minutes to allow Senator FEINSTEIN and me to thank our colleagues for their help over the last several days as we have worked through the cyber bill.

I thank my vice chairman, who has been beside me all the way, and I thank Chairman JOHNSON and Ranking Member CARPER for the input they provided.

I want to say to committee staff who has worked night and day to get us to this point and to members of the committee who worked diligently for months to get this legislation enacted that I could not have done it without you.

Now the work begins as we go to conference.

I turn to the vice chairman.

Mrs. FEINSTEIN. I thank you very much.

Madam President, I just want to say a personal word to Chairman BURR, and maybe it is to everyone in this body. One of the things I have learned from two prior cyber bills is that if you really want to get a bill done, it has to be bipartisan, particularly a bill that is technical, difficult, and hard to put together, and a bill where often there are two sides. I thank you for recognizing this. We stood shoulder to shoulder and the right things happened, and now we can go to conference.

I also want to say that we did everything in this bill we possibly could to satisfy what were legitimate privacy concerns. The managers' package had 14 such amendments, and before that our staffs sat down with a number of proposals from Senators and went over literally dozens of additional amendments. So we took what we could.

When the chairman talks about the balance, what he means is that this is the first time the chamber of commerce has supported a bipartisan bill. This is the first time we had virtually all the big employers—banks and retailers and other companies—supporting a bipartisan bill because today everybody understands what the problem of cybersecurity is much greater. So we stood shoulder to shoulder, and you all responded, and I am very grateful.

There is still a lot of work to be done, but, Mr. Chairman, you and your staff have been terrific. I would like to single a couple of them out, if I might, in particular, Chris Joyner, Michael Geffroy, Jack Livingston, Janet Fisher, John Matchison, and Walter Weiss.

I also want to thank TOM CARPER, who has been working to get this bill passed as much as anyone. He wrote one of the key changes in the managers' package to improve privacy as information moves through the DHS portal. He was supported by his chairman, Senator JOHNSON. He has been a close partner throughout the process, and I thank him.

I also thank Gabbie Batkin, Matt Grote, and the other members of Senator CARPER's staff.

We had incredible support from our committee. It is a committee of 15—8 Republicans and 7 Democrats. I thank Senator COLLINS, who was particularly concerned about the critical infrastructure of this country, as well as Senators MIKULSKI, WHITEHOUSE, KING, WARNER, HEINRICH, BLUNT, NELSON, and COATS. I know they will help us push this bill forward as we go to conference with the House.

I greatly appreciate the supporters of this bill outside the Senate, to include the U.S. chamber of commerce and the associations that have endorsed this bill, tech companies like IBM and Oracle, Secretary Jeh Johnson at the Department of Homeland Security, and NSA Directors Keith Alexander and MIKE ROGERS, and Lisa Monaco and Michael Daniel at the White House.

On my staff, I would like to thank David Grannis, our staff director on the minority side. David has been there for these previous cyber bills, and it has proven to be a very difficult issue. David, you are a 10.

I also thank Josh Alexander. Josh has been our lead drafter and negotiator and knows these cyber issues better than anyone. He has been tireless on reaching agreement after agreement on this bill, and is, as much as anybody, responsible for today's vote.

I would also like to thank my former cyber staffer Andy Grotto, as well as Mike Buchwald, Brett Freedman, Nate Adler, and Nick Basciano. Thank you all so very much.

Finally, I very much appreciate the work done by Ayesha Khanna in the Democratic leader's office and Jeffrey Ratner at the White House.

We have the administration behind the bill, we have the Department of Homeland Security behind the bill, and we have the editorial pages of the Washington Post and the Wall Street Journal, as well as the chamber of commerce, and most of the businesses of America.

So, Mr. Chairman, you did a great job, and thank you from the bottom of my heart.

The PRESIDING OFFICER. The majority leader.

Mr. MCCONNELL. Madam President, I just want to add my words of congratulation to Chairman BURR and Ranking Member FEINSTEIN. This is a

very complicated issue, as we all know. It has been around multiple Congresses, and it took their leadership and coordination and cooperation first to produce a 14-to-1 vote in the committee and then this extraordinary success we have had out here on the floor. I know all of us are extremely proud of the great work you have done.

Congratulations. We deeply appreciate the contribution you have made to our country.

The PRESIDING OFFICER. The bill having been read the third time, the question is, Shall it pass?

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

The PRESIDING OFFICER. Is there a sufficient second?

There is 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 74, nays 21, as follows:

[Rollcall Vote No. 291 Leg.]

YEAS—74

Alexander	Fischer	Murphy
Ayotte	Flake	Murray
Barrasso	Gardner	Nelson
Bennet	Gillibrand	Perdue
Blumenthal	Grassley	Peters
Blunt	Hatch	Portman
Boozman	Heinrich	Reed
Boxer	Heitkamp	Reid
Burr	Hirono	Roberts
Cantwell	Hoeven	Rounds
Capito	Inhofe	Sasse
Carper	Isakson	Schatz
Casey	Johnson	Schumer
Cassidy	Kaine	Scott
Coats	King	Sessions
Cochran	Kirk	Shaheen
Collins	Klobuchar	Shelby
Corker	Lankford	Stabenow
Cornyn	Manchin	Thune
Cotton	McCain	Tillis
Donnelly	McCaskill	Toomey
Durbin	McConnell	Warner
Enzi	Mikulski	Whitehouse
Ernst	Moran	Wicker
Feinstein	Murkowski	

NAYS—21

Baldwin	Franken	Risch
Booker	Heller	Sanders
Brown	Leahy	Sullivan
Cardin	Lee	Tester
Coons	Markey	Udall
Crapo	Menendez	Warren
Daines	Merkley	Wyden

NOT VOTING—5

Cruz	Paul	Vitter
Graham	Rubio	

The bill (S. 754), as amended, was passed, as follows:

S. 754

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. TABLE OF CONTENTS.

The table of contents of this Act is as follows:

Sec. 1. Table of contents.

TITLE I—CYBERSECURITY INFORMATION SHARING

Sec. 101. Short title.
Sec. 102. Definitions.
Sec. 103. Sharing of information by the Federal Government.
Sec. 104. Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats.
Sec. 105. Sharing of cyber threat indicators and defensive measures with the Federal Government.
Sec. 106. Protection from liability.
Sec. 107. Oversight of Government activities.
Sec. 108. Construction and preemption.
Sec. 109. Report on cybersecurity threats.
Sec. 110. Conforming amendment.

TITLE II—FEDERAL CYBERSECURITY ENHANCEMENT

Sec. 201. Short title.
Sec. 202. Definitions.
Sec. 203. Improved Federal network security.
Sec. 204. Advanced internal defenses.
Sec. 205. Federal cybersecurity requirements.
Sec. 206. Assessment; reports.
Sec. 207. Termination.
Sec. 208. Identification of information systems relating to national security.
Sec. 209. Direction to agencies.

TITLE III—FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT

Sec. 301. Short title.
Sec. 302. Definitions.
Sec. 303. National cybersecurity workforce measurement initiative.
Sec. 304. Identification of cyber-related roles of critical need.
Sec. 305. Government Accountability Office status reports.

TITLE IV—OTHER CYBER MATTERS

Sec. 401. Study on mobile device security.
Sec. 402. Department of State international cyberspace policy strategy.
Sec. 403. Apprehension and prosecution of international cyber criminals.
Sec. 404. Enhancement of emergency services.
Sec. 405. Improving cybersecurity in the health care industry.
Sec. 406. Federal computer security.
Sec. 407. Strategy to protect critical infrastructure at greatest risk.
Sec. 408. Stopping the fraudulent sale of financial information of people of the United States.
Sec. 409. Effective period.

TITLE I—CYBERSECURITY INFORMATION SHARING

SEC. 101. SHORT TITLE.

This title may be cited as the ''Cybersecurity Information Sharing Act of 2015''.

SEC. 102. DEFINITIONS.

In this title:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(2) ANTITRUST LAWS.—The term ''antitrust laws''—

(A) has the meaning given the term in section 1 of the Clayton Act (15 U.S.C. 12);

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and

(C) includes any State law that has the same intent and effect as the laws under subparagraphs (A) and (B).

(3) APPROPRIATE FEDERAL ENTITIES.—The term ''appropriate Federal entities'' means the following:

(A) The Department of Commerce.

(B) The Department of Defense.

(C) The Department of Energy.

(D) The Department of Homeland Security.

(E) The Department of Justice.

(F) The Department of the Treasury.

(G) The Office of the Director of National Intelligence.

(4) CYBERSECURITY PURPOSE.—The term ''cybersecurity purpose'' means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

(5) CYBERSECURITY THREAT.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term ''cybersecurity threat'' means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

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

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

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

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

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

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

(E) malicious cyber command and control;

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

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

(H) any combination thereof.

(7) DEFENSIVE MEASURE.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term ''defensive measure'' means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

(B) EXCLUSION.—The term ''defensive measure'' does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or data on an information system not belonging to—

(i) the private entity operating the measure; or

(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

(8) ENTITY.—

(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term ''entity'' means any private entity, non-Federal government agency or department, or State,

tribal, or local government (including a political subdivision, department, or component thereof).

(B) INCLUSIONS.—The term ''entity'' includes a government agency or department of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(C) EXCLUSION.—The term ''entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(9) FEDERAL ENTITY.—The term ''Federal entity'' means a department or agency of the United States or any component of such department or agency.

(10) INFORMATION SYSTEM.—The term ''information system''—

(A) has the meaning given the term in section 3502 of title 44, United States Code; and

(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

(11) LOCAL GOVERNMENT.—The term ''local government'' means any borough, city, county, parish, town, township, village, or other political subdivision of a State.

(12) MALICIOUS CYBER COMMAND AND CONTROL.—The term ''malicious cyber command and control'' means a method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

(13) MALICIOUS RECONNAISSANCE.—The term ''malicious reconnaissance'' means a method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(14) MONITOR.—The term ''monitor'' means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

(15) PRIVATE ENTITY.—

(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term ''private entity'' means any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof.

(B) INCLUSION.—The term ''private entity'' includes a State, tribal, or local government performing electric or other utility services.

(C) EXCLUSION.—The term ''private entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(16) SECURITY CONTROL.—The term ''security control'' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

(17) SECURITY VULNERABILITY.—The term ''security vulnerability'' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

(18) TRIBAL.—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SEC. 103. SHARING OF INFORMATION BY THE FEDERAL GOVERNMENT.

(a) IN GENERAL.—Consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate Federal entities, shall develop and promulgate procedures to facilitate and promote—

(1) the timely sharing of classified cyber threat indicators in the possession of the Federal Government with cleared representatives of relevant entities;

(2) the timely sharing with relevant entities of cyber threat indicators or information in the possession of the Federal Government that may be declassified and shared at an unclassified level;

(3) the sharing with relevant entities, or the public if appropriate, of unclassified, including controlled unclassified, cyber threat indicators in the possession of the Federal Government;

(4) the sharing with entities, if appropriate, of information in the possession of the Federal Government about cybersecurity threats to such entities to prevent or mitigate adverse effects from such cybersecurity threats; and

(5) the periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analysis of cyber threat indicators and information in possession of the Federal Government, with attention to accessibility and implementation challenges faced by small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 632)).

(b) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed and promulgated under subsection (a) shall—

(A) ensure the Federal Government has and maintains the capability to share cyber threat indicators in real time consistent with the protection of classified information;

(B) incorporate, to the greatest extent practicable, existing processes and existing roles and responsibilities of Federal and non-Federal entities for information sharing by the Federal Government, including sector specific information sharing and analysis centers;

(C) include procedures for notifying, in a timely manner, entities that have received a cyber threat indicator from a Federal entity under this title that is known or determined to be in error or in contravention of the requirements of this title or another provision of Federal law or policy of such error or contravention;

(D) include requirements for Federal entities sharing cyber threat indicators or defensive measures to implement and utilize security controls to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures;

(E) include procedures that require a Federal entity, prior to the sharing of a cyber threat indicator—

(i) to review such cyber threat indicator to assess whether such cyber threat indicator contains any information that such Federal entity knows at the time of sharing to be personal information or information that identifies a specific person not directly related to a cybersecurity threat and remove such information; or

(ii) to implement and utilize a technical capability configured to remove any personal information or information that identifies a specific person not directly related to a cybersecurity threat; and

(F) include procedures for notifying, in a timely manner, any United States person whose personal information is known or determined to have been shared by a Federal entity in violation of this Act.

(2) COORDINATION.—In developing the procedures required under this section, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General shall coordinate with appropriate Federal entities, including the Small Business Administration and the National Laboratories (as defined in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801)), to ensure that effective protocols are implemented that will facilitate and promote the sharing of cyber threat indicators by the Federal Government in a timely manner.

(c) SUBMITTAL TO CONGRESS.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of the appropriate Federal entities, shall submit to Congress the procedures required by subsection (a).

SEC. 104. AUTHORIZATIONS FOR PREVENTING, DETECTING, ANALYZING, AND MITIGATING CYBERSECURITY THREATS.

(a) AUTHORIZATION FOR MONITORING.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, monitor—

(A) an information system of such private entity;

(B) an information system of another entity, upon the authorization and written consent of such other entity;

(C) an information system of a Federal entity, upon the authorization and written consent of an authorized representative of the Federal entity; and

(D) information that is stored on, processed by, or transiting an information system monitored by the private entity under this paragraph.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the monitoring of an information system, or the use of any information obtained through such monitoring, other than as provided in this title; or

(B) to limit otherwise lawful activity.

(b) AUTHORIZATION FOR OPERATION OF DEFENSIVE MEASURES.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, operate a defensive measure that is applied to—

(A) an information system of such private entity in order to protect the rights or property of the private entity;

(B) an information system of another entity upon written consent of such entity for operation of such defensive measure to protect the rights or property of such entity; and

(C) an information system of a Federal entity upon written consent of an authorized representative of such Federal entity for operation of such defensive measure to protect the rights or property of the Federal Government.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the use of a defensive measure other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

(c) AUTHORIZATION FOR SHARING OR RECEIVING CYBER THREAT INDICATORS OR DEFENSIVE MEASURES.—

(1) IN GENERAL.—Except as provided in paragraph (2) and notwithstanding any other provision of law, an entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other entity or the Federal Government a cyber threat indicator or defensive measure.

(2) LAWFUL RESTRICTION.—An entity receiving a cyber threat indicator or defensive measure from another entity or Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator or defensive

measure by the sharing entity or Federal entity.

(3) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the sharing or receiving of a cyber threat indicator or defensive measure other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

(d) PROTECTION AND USE OF INFORMATION.—

(1) SECURITY OF INFORMATION.—An entity monitoring an information system, operating a defensive measure, or providing or receiving a cyber threat indicator or defensive measure under this section shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicator or defensive measure.

(2) REMOVAL OF CERTAIN PERSONAL INFORMATION.—An entity sharing a cyber threat indicator pursuant to this title shall, prior to such sharing—

(A) review such cyber threat indicator to assess whether such cyber threat indicator contains any information that the entity knows at the time of sharing to be personal information or information that identifies a specific person not directly related to a cybersecurity threat and remove such information; or

(B) implement and utilize a technical capability configured to remove any information contained within such indicator that the entity knows at the time of sharing to be personal information or information that identifies a specific person not directly related to a cybersecurity threat.

(3) USE OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY ENTITIES.—

(A) IN GENERAL.—Consistent with this title, a cyber threat indicator or defensive measure shared or received under this section may, for cybersecurity purposes—

(i) be used by an entity to monitor or operate a defensive measure that is applied to—

(I) an information system of the entity; or

(II) an information system of another entity or a Federal entity upon the written consent of that other entity or that Federal entity; and

(ii) be otherwise used, retained, and further shared by an entity subject to—

(I) an otherwise lawful restriction placed by the sharing entity or Federal entity on such cyber threat indicator or defensive measure; or

(II) an otherwise applicable provision of law.

(B) CONSTRUCTION.—Nothing in this paragraph shall be construed to authorize the use of a cyber threat indicator or defensive measure other than as provided in this section.

(4) USE OF CYBER THREAT INDICATORS BY STATE, TRIBAL, OR LOCAL GOVERNMENT.—

(A) LAW ENFORCEMENT USE.—

(i) PRIOR WRITTEN CONSENT.—Except as provided in clause (ii), a cyber threat indicator shared with a State, tribal, or local government under this section may, with the prior written consent of the entity sharing such indicator, be used by a State, tribal, or local government for the purpose of preventing, investigating, or prosecuting any of the offenses described in section 105(d)(5)(A)(vi).

(ii) ORAL CONSENT.—If exigent circumstances prevent obtaining written consent under clause (i), such consent may be provided orally with subsequent documentation of the consent.

(B) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator shared with a State, tribal, or local government under this section shall be—

(i) deemed voluntarily shared information; and

(ii) exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records.

(C) STATE, TRIBAL, AND LOCAL REGULATORY AUTHORITY.—

(i) IN GENERAL.—Except as provided in clause (ii), a cyber threat indicator or defensive measure shared with a State, tribal, or local government under this title shall not be directly used by any State, tribal, or local government to regulate, including an enforcement action, the lawful activity of any entity, including an activity relating to monitoring, operating a defensive measure, or sharing of a cyber threat indicator.

(ii) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—A cyber threat indicator or defensive measure shared as described in clause (i) may, consistent with a State, tribal, or local government regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of a regulation relating to such information systems.

(e) ANTITRUST EXEMPTION.—

(1) IN GENERAL.—Except as provided in section 108(e), it shall not be considered a violation of any provision of antitrust laws for 2 or more private entities to exchange or provide a cyber threat indicator, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat, for cybersecurity purposes under this title.

(2) APPLICABILITY.—Paragraph (1) shall apply only to information that is exchanged or assistance provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system; or

(B) communicating or disclosing a cyber threat indicator to help prevent, investigate, or mitigate the effect of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system.

(f) NO RIGHT OR BENEFIT.—The sharing of a cyber threat indicator with an entity under this title shall not create a right or benefit to similar information by such entity or any other entity.

SEC. 105. SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH THE FEDERAL GOVERNMENT.

(a) REQUIREMENT FOR POLICIES AND PROCEDURES.—

(1) INTERIM POLICIES AND PROCEDURES.—Not later than 60 days after the date of the enactment of this Act, the Attorney General and the Secretary of Homeland Security shall, in coordination with the heads of the appropriate Federal entities, develop and submit to Congress interim policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government.

(2) FINAL POLICIES AND PROCEDURES.—Not later than 180 days after the date of the enactment of this Act, the Attorney General and the Secretary of Homeland Security shall, in coordination with the heads of the appropriate Federal entities, promulgate final policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government.

(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 only subject to a delay, modification, or other action due to controls established for such real-time process that could impede real-time receipt by all of the appropriate Federal entities when the delay, modification, or other action is due to controls—

(I) agreed upon unanimously by all of the heads of the appropriate Federal entities;

(II) carried out before any of the appropriate Federal entities retains or uses the cyber threat indicators or defensive measures; and

(III) uniformly applied such that each of the appropriate Federal entities is subject to the same delay, modification, or other action; 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) ensures that all of the appropriate Federal entities receive in an automated manner such cyber threat indicators shared through the real-time process within the Department of Homeland Security;

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

(E) 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 in real time with receipt through the process within the Department of Homeland Security.

(4) OTHER FEDERAL ENTITIES.—The process developed and implemented under paragraph (1) shall ensure that other Federal entities receive in a timely manner any cyber threat indicators and defensive measures shared with the Federal Government through such process.

(5) REPORT ON DEVELOPMENT AND IMPLEMENTATION.—

(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a report on the development and implementation of the capability and process required by paragraph (1), including a description of such capability and process and the public notice of, and access to, such process.

(B) CLASSIFIED ANNEX.—The report required by subparagraph (A) shall be submitted in unclassified form, but may include a classified annex.

(d) INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.—

(1) NO WAIVER OF PRIVILEGE OR PROTECTION.—The provision of cyber threat indicators and defensive measures to the Federal Government under this title shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

(2) PROPRIETARY INFORMATION.—Consistent with section 104(c)(2), a cyber threat indicator or defensive measure provided by an entity to the Federal Government under this title shall be considered the commercial, financial, and proprietary information of such entity when so designated by the originating entity or a third party acting in accordance with the written authorization of the originating entity.

(3) EXEMPTION FROM DISCLOSURE.—Cyber threat indicators and defensive measures provided to the Federal Government under this title shall be—

(A) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records; and

(B) withheld, without discretion, from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local provision of law requiring disclosure of information or records.

(4) EX PARTE COMMUNICATIONS.—The provision of a cyber threat indicator or defensive measure to the Federal Government under this title shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

(5) DISCLOSURE, RETENTION, AND USE.—

(A) AUTHORIZED ACTIVITIES.—Cyber threat indicators and defensive measures provided to the Federal Government under this title may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

(i) a cybersecurity purpose;

(ii) the purpose of identifying a cybersecurity threat, including the source of such cybersecurity threat, or a security vulnerability;

(iii) the purpose of identifying a cybersecurity threat involving the use of an information system by a foreign adversary or terrorist;

(iv) the purpose of responding to, or otherwise preventing or mitigating, an imminent threat of death, serious bodily harm, or serious economic harm, including a terrorist act or a use of a weapon of mass destruction;

(v) the purpose of responding to, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(vi) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in clause (iv) or any of the offenses listed in—

(I) sections 1028 through 1030 of title 18, United States Code (relating to fraud and identity theft);

(II) chapter 37 of such title (relating to espionage and censorship); and

(III) chapter 90 of such title (relating to protection of trade secrets).

(B) PROHIBITED ACTIVITIES.—Cyber threat indicators and defensive measures provided to the Federal Government under this title shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under subparagraph (A).

(C) PRIVACY AND CIVIL LIBERTIES.—Cyber threat indicators and defensive measures provided to the Federal Government under this title shall be retained, used, and disseminated by the Federal Government—

(i) in accordance with the policies, procedures, and guidelines required by subsections (a) and (b);

(ii) in a manner that protects from unauthorized use or disclosure any cyber threat indicators that may contain personal information or information that identifies specific persons; and

(iii) in a manner that protects the confidentiality of cyber threat indicators containing personal information or information that identifies a specific person.

(D) FEDERAL REGULATORY AUTHORITY.—

(i) IN GENERAL.—Except as provided in clause (ii), cyber threat indicators and defensive measures provided to the Federal Government under this title shall not be directly used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any entity, including activities relating to monitoring, operating defensive measures, or sharing cyber threat indicators.

(ii) EXCEPTIONS.—

(I) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—Cyber threat indicators and defensive measures provided to the Federal Government under this title may, consistent with Federal or State regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such information systems.

(II) PROCEDURES DEVELOPED AND IMPLEMENTED UNDER THIS TITLE.—Clause (i) shall not apply to procedures developed and implemented under this title.

SEC. 106. PROTECTION FROM LIABILITY.

(a) MONITORING OF INFORMATION SYSTEMS.—No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of information systems and information under section 104(a) that is conducted in accordance with this title.

(b) SHARING OR RECEIPT OF CYBER THREAT INDICATORS.—No cause of action shall lie or be maintained in any court against any entity, and such action shall be promptly dismissed, for the sharing or receipt of cyber threat indicators or defensive measures under section 104(c) if—

(1) such sharing or receipt is conducted in accordance with this title; and

(2) in a case in which a cyber threat indicator or defensive measure is shared with the Federal Government, the cyber threat indicator or defensive measure is shared in a manner that is consistent with section 105(c)(1)(B) and the sharing or receipt, as the case may be, occurs after the earlier of—

(A) the date on which the interim policies and procedures are submitted to Congress under section 105(a)(1) and guidelines are submitted to Congress under section 105(b)(1); or

(B) the date that is 60 days after the date of the enactment of this Act.

(c) CONSTRUCTION.—Nothing in this section shall be construed—

(1) to require dismissal of a cause of action against an entity that has engaged in gross negligence or willful misconduct in the course of conducting activities authorized by this title; or

(2) to undermine or limit the availability of otherwise applicable common law or statutory defenses.

SEC. 107. OVERSIGHT OF GOVERNMENT ACTIVITIES.

(a) BIENNIAL REPORT ON IMPLEMENTATION.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, and not less frequently than once every 2 years thereafter, the heads of the appropriate Federal entities shall jointly submit and the Inspector General of the Department of Homeland Security, the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, the Inspector General of the Department of Defense, and the Inspector General of the Department of Energy, in consultation with the Council of Inspectors General on Financial Oversight, shall jointly submit to Congress a detailed report concerning the implementation of this title during—

(A) in the case of the first report submitted under this paragraph, the most recent 1-year period; and

(B) in the case of any subsequent report submitted under this paragraph, the most recent 2-year period.

(2) CONTENTS.—Each report submitted under paragraph (1) shall include, for the period covered by the report, the following:

(A) An assessment of the sufficiency of the policies, procedures, and guidelines required by section 105 in ensuring that cyber threat indicators are shared effectively and responsibly within the Federal Government.

(B) An evaluation of the effectiveness of real-time information sharing through the capability and process developed under section 105(c), including any impediments to such real-time sharing.

(C) An assessment of the sufficiency of the procedures developed under section 103 in ensuring that cyber threat indicators in the possession of the Federal Government are shared in a timely and adequate manner with appropriate entities, or, if appropriate, are made publicly available.

(D) An assessment of whether cyber threat indicators have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purposes of this title.

(E) A review of the type of cyber threat indicators shared with the appropriate Federal entities under this title, including the following:

(i) The number of cyber threat indicators received through the capability and process developed under section 105(c).

(ii) The number of times that information shared under this title was used by a Federal entity to prosecute an offense consistent with section 105(d)(5)(A).

(iii) The degree to which such information may affect the privacy and civil liberties of specific persons.

(iv) A quantitative and qualitative assessment of the effect of the sharing of such cyber threat indicators with the Federal Government on privacy and civil liberties of specific persons, including the number of notices that were issued with respect to a failure to remove personal information or information that identified a specific person not directly related to a cybersecurity threat in accordance with the procedures required by section 105(b)(3)(D).

(v) The adequacy of any steps taken by the Federal Government to reduce such effect.

(F) A review of actions taken by the Federal Government based on cyber threat indicators shared with the Federal Government under this title, including the appropriateness of any subsequent use or dissemination of such cyber threat indicators by a Federal entity under section 105.

(G) A description of any significant violations of the requirements of this title by the Federal Government.

(H) A summary of the number and type of entities that received classified cyber threat indicators from the Federal Government under this title and an evaluation of the risks and benefits of sharing such cyber threat indicators.

(3) RECOMMENDATIONS.—Each report submitted under paragraph (1) may include recommendations for improvements or modifications to the authorities and processes under this title.

(4) FORM OF REPORT.—Each report required by paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(b) REPORTS ON PRIVACY AND CIVIL LIBERTIES.—

(1) BIENNIAL REPORT FROM PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD.—Not later than 2 years after the date of the enactment of this Act and not less frequently than once every 2 years thereafter, the Privacy and Civil Liberties Oversight Board shall submit to Congress and the President a report providing—

(A) an assessment of the effect on privacy and civil liberties by the type of activities carried out under this title; and

(B) an assessment of the sufficiency of the policies, procedures, and guidelines established pursuant to section 105 in addressing concerns relating to privacy and civil liberties.

(2) BIENNIAL REPORT OF INSPECTORS GENERAL.—

(A) IN GENERAL.—Not later than 2 years after the date of the enactment of this Act and not less frequently than once every 2 years thereafter, the Inspector General of the Department of Homeland Security, the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, the Inspector General of the Department of Defense, and the Inspector General of the Department of Energy shall, in consultation with the Council of Inspectors General on Financial Oversight, jointly submit to Congress a report on the receipt, use, and dissemination of cyber threat indicators and defensive measures that have been shared with Federal entities under this title.

(B) CONTENTS.—Each report submitted under subparagraph (A) shall include the following:

(i) A review of the types of cyber threat indicators shared with Federal entities.

(ii) A review of the actions taken by Federal entities as a result of the receipt of such cyber threat indicators.

(iii) A list of Federal entities receiving such cyber threat indicators.

(iv) A review of the sharing of such cyber threat indicators among Federal entities to identify inappropriate barriers to sharing information.

(3) RECOMMENDATIONS.—Each report submitted under this subsection may include such recommendations as the Privacy and Civil Liberties Oversight Board, with respect to a report submitted under paragraph (1), or the Inspectors General referred to in paragraph (2)(A), with respect to a report submitted under paragraph (2), may have for improvements or modifications to the authorities under this title.

(4) FORM.—Each report required under this subsection shall be submitted in unclassified form, but may include a classified annex.

SEC. 108. CONSTRUCTION AND PREEMPTION.

(a) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this title shall be construed—

(1) to limit or prohibit otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity, by an entity to any other entity or the Federal Government under this title; or

(2) to limit or prohibit otherwise lawful use of such disclosures by any Federal entity, even when such otherwise lawful disclosures duplicate or replicate disclosures made under this title.

(b) WHISTLE BLOWER PROTECTIONS.—Nothing in this title shall be construed to prohibit or limit the disclosure of information protected under section 2302(b)(8) of title 5, United States Code (governing disclosures of illegality, waste, fraud, abuse, or public health or safety threats), section 7211 of title 5, United States Code (governing disclosures to Congress), section 1034 of title 10, United States Code (governing disclosure to Congress by members of the military), section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) (governing disclosure by employees of elements of the intelligence community), or any similar provision of Federal or State law.

(c) PROTECTION OF SOURCES AND METHODS.—Nothing in this title shall be construed—

(1) as creating any immunity against, or otherwise affecting, any action brought by the Federal Government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, or use of classified information;

(2) to affect the conduct of authorized law enforcement or intelligence activities; or

(3) to modify the authority of a department or agency of the Federal Government to protect classified information and sources and methods and the national security of the United States.

(d) RELATIONSHIP TO OTHER LAWS.—Nothing in this title shall be construed to affect any requirement under any other provision of law for an entity to provide information to the Federal Government.

(e) PROHIBITED CONDUCT.—Nothing in this title shall be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

(f) INFORMATION SHARING RELATIONSHIPS.—Nothing in this title shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any entity and another entity or a Federal entity; or

(4) to require the use of the capability and process within the Department of Homeland Security developed under section 105(c).

(g) PRESERVATION OF CONTRACTUAL OBLIGATIONS AND RIGHTS.—Nothing in this title shall be construed—

(1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any entities, or between any entity and a Federal entity; or

(2) to abrogate trade secret or intellectual property rights of any entity or Federal entity.

(h) ANTI-TASKING RESTRICTION.—Nothing in this title shall be construed to permit a Federal entity—

(1) to require an entity to provide information to a Federal entity or another entity;

(2) to condition the sharing of cyber threat indicators with an entity on such entity's provision of cyber threat indicators to a Federal entity or another entity; or

(3) to condition the award of any Federal grant, contract, or purchase on the provision of a cyber threat indicator to a Federal entity or another entity.

(i) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this title shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized in this title.

(j) USE AND RETENTION OF INFORMATION.—Nothing in this title shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use any information shared under this title for any use other than permitted in this title.

(k) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This title supersedes any statute or other provision of law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this title.

(2) STATE LAW ENFORCEMENT.—Nothing in this title shall be construed to supersede any statute or other provision of law of a State or political subdivision of a State concerning the use of authorized law enforcement practices and procedures.

(l) REGULATORY AUTHORITY.—Nothing in this title shall be construed—

(1) to authorize the promulgation of any regulations not specifically authorized by this title;

(2) to establish or limit any regulatory authority not specifically established or limited under this title; or

(3) to authorize regulatory actions that would duplicate or conflict with regulatory requirements, mandatory standards, or related processes under another provision of Federal law.

(m) AUTHORITY OF SECRETARY OF DEFENSE TO RESPOND TO CYBER ATTACKS.—Nothing in this title shall be construed to limit the authority of the Secretary of Defense to develop, prepare, coordinate, or, when authorized by the President to do so, conduct a military cyber operation in response to a malicious cyber activity carried out against the United States or a United States person by a foreign government or an organization sponsored by a foreign government or a terrorist organization.

SEC. 109. REPORT ON CYBERSECURITY THREATS.

(a) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the heads of other appropriate elements of the intelligence community, shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on cybersecurity threats, including cyber attacks, theft, and data breaches.

(b) CONTENTS.—The report required by subsection (a) shall include the following:

(1) An assessment of the current intelligence sharing and cooperation relationships of the United States with other countries regarding cybersecurity threats, including cyber attacks, theft, and data breaches, directed against the United States and which threaten the United States national security interests and economy and intellectual property, specifically identifying the relative utility of such relationships, which elements of the intelligence community participate in such relationships, and whether and how such relationships could be improved.

(2) A list and an assessment of the countries and nonstate actors that are the primary threats of carrying out a cybersecurity threat, including a cyber attack, theft, or data breach, against the United States and which threaten the United States national security, economy, and intellectual property.

(3) A description of the extent to which the capabilities of the United States Government to respond to or prevent cybersecurity threats, including cyber attacks, theft, or data breaches, directed against the United States private sector are degraded by a delay in the prompt notification by private entities of such threats or cyber attacks, theft, and breaches.

(4) An assessment of additional technologies or capabilities that would enhance the ability of the United States to prevent and to respond to cybersecurity threats, including cyber attacks, theft, and data breaches.

(5) An assessment of any technologies or practices utilized by the private sector that could be rapidly fielded to assist the intelligence community in preventing and responding to cybersecurity threats.

(c) ADDITIONAL REPORT.—At the time the report required by subsection (a) is submitted, the Director of National Intelligence shall submit to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives a report containing the information required by subsection (b)(2).

(d) FORM OF REPORT.—The report required by subsection (a) shall be made available in classified and unclassified forms.

(e) INTELLIGENCE COMMUNITY DEFINED.—In this section, the term ''intelligence community'' has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

SEC. 110. CONFORMING AMENDMENT.

Section 941(c)(3) of the National Defense Authorization Act for Fiscal Year 2013 (Public Law 112–239; 10 U.S.C. 2224 note) is amended by inserting at the end the following: ''The Secretary may share such information with other Federal entities if such information consists of cyber threat indicators and defensive measures and such information is shared consistent with the policies and procedures promulgated by the Attorney General and the Secretary of Homeland Security under section 105 of the Cybersecurity Information Sharing Act of 2015.''.

TITLE II—FEDERAL CYBERSECURITY ENHANCEMENT

SEC. 201. SHORT TITLE.

This title may be cited as the ''Federal Cybersecurity Enhancement Act of 2015''.

SEC. 202. DEFINITIONS.

In this title—

(1) the term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code;

(2) the term ''agency information system'' has the meaning given the term in section 228 of the Homeland Security Act of 2002, as added by section 203(a);

(3) the term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Homeland Security of the House of Representatives;

(4) the terms ''cybersecurity risk'' and ''information system'' have the meanings given those terms in section 227 of the Homeland Security Act of 2002, as so redesignated by section 203(a);

(5) the term ''Director'' means the Director of the Office of Management and Budget;

(6) the term ''intelligence community'' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4));

(7) the term ''national security system'' has the meaning given the term in section 11103 of title 40, United States Code; and

(8) the term ''Secretary'' means the Secretary of Homeland Security.

SEC. 203. IMPROVED FEDERAL NETWORK SECURITY.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended—

(1) by redesignating section 228 as section 229;

(2) by redesignating section 227 as subsection (c) of section 228, as added by paragraph (4), and adjusting the margins accordingly;

(3) by redesignating the second section designated as section 226 (relating to the national cybersecurity and communications integration center) as section 227;

(4) by inserting after section 227, as so redesignated, the following:

''SEC. 228. CYBERSECURITY PLANS.

''(a) DEFINITIONS.—In this section—

''(1) the term 'agency information system' means an information system used or operated by an agency or by another entity on behalf of an agency;

''(2) the terms 'cybersecurity risk' and 'information system' have the meanings given those terms in section 227;

''(3) the term 'intelligence community' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)); and

''(4) the term 'national security system' has the meaning given the term in section 11103 of title 40, United States Code.

''(b) INTRUSION ASSESSMENT PLAN.—

''(1) REQUIREMENT.—The Secretary, in coordination with the Director of the Office of Management and Budget, shall develop and implement an intrusion assessment plan to identify and remove intruders in agency information systems.

''(2) EXCEPTION.—The intrusion assessment plan required under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.'';

(5) in section 228(c), as so redesignated, by striking ''section 226'' and inserting ''section 227''; and

(6) by inserting after section 229, as so redesignated, the following:

''SEC. 230. FEDERAL INTRUSION DETECTION AND PREVENTION SYSTEM.

''(a) DEFINITIONS.—In this section—

''(1) the term 'agency' has the meaning given that term in section 3502 of title 44, United States Code;

''(2) the term 'agency information' means information collected or maintained by or on behalf of an agency;

''(3) the term 'agency information system' has the meaning given the term in section 228; and

''(4) the terms 'cybersecurity risk' and 'information system' have the meanings given those terms in section 227.

''(b) REQUIREMENT.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of this section, the Secretary shall deploy, operate, and maintain, to make available for use by any agency, with or without reimbursement—

''(A) a capability to detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system; and

''(B) a capability to prevent network traffic associated with such cybersecurity risks from transiting or traveling to or from an agency information system or modify such network traffic to remove the cybersecurity risk.

''(2) REGULAR IMPROVEMENT.—The Secretary shall regularly deploy new technologies and modify existing technologies to the intrusion detection and prevention capabilities described in paragraph (1) as appropriate to improve the intrusion detection and prevention capabilities.

''(c) ACTIVITIES.—In carrying out subsection (b), the Secretary—

''(1) may access, and the head of an agency may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information transiting or traveling to or from an agency information system, regardless of the location from which the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or prevent the head of an agency from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);

''(2) may enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy and operate technologies in accordance with subsection (b);

''(3) may retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect information and information systems from cybersecurity risks;

''(4) shall regularly assess through operational test and evaluation in real world or simulated environments available advanced protective technologies to improve detection and prevention capabilities, including commercial and non-commercial technologies and detection technologies beyond signature-based detection, and utilize such technologies when appropriate;

''(5) shall establish a pilot to acquire, test, and deploy, as rapidly as possible, technologies described in paragraph (4);

''(6) shall periodically update the privacy impact assessment required under section 208(b) of the E-Government Act of 2002 (44 U.S.C. 3501 note); and

''(7) shall ensure that—

''(A) activities carried out under this section are reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

''(B) information accessed by the Secretary will be retained no longer than reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

''(C) notice has been provided to users of an agency information system concerning access to communications of users of the agency information system for the purpose of protecting agency information and the agency information system; and

''(D) the activities are implemented pursuant to policies and procedures governing the operation of the intrusion detection and prevention capabilities.

''(d) PRIVATE ENTITIES.—

''(1) CONDITIONS.—A private entity described in subsection (c)(2) may not—

''(A) disclose any network traffic transiting or traveling to or from an agency information system to any entity without the consent of the Department or the agency that disclosed the information under subsection (c)(1); or

''(B) use any network traffic transiting or traveling to or from an agency information system to which the private entity gains access in accordance with this section for any purpose other than to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to subsection (c)(2) or as part of another contract with the Secretary.

''(2) LIMITATION ON LIABILITY.—No cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to subsection (c)(2).

''(3) RULE OF CONSTRUCTION.—Nothing in paragraph (2) shall be construed to authorize an Internet service provider to break a user agreement with a customer without the consent of the customer.

''(e) ATTORNEY GENERAL REVIEW.—Not later than 1 year after the date of enactment of this section, the Attorney General shall review the policies and guidelines for the program carried out under this section to ensure that the policies and guidelines are consistent with applicable law governing the acquisition, interception, retention, use, and disclosure of communications.''.

(b) PRIORITIZING ADVANCED SECURITY TOOLS.—The Director and the Secretary, in consultation with appropriate agencies, shall—

(1) review and update governmentwide policies and programs to ensure appropriate prioritization and use of network security monitoring tools within agency networks; and

(2) brief appropriate congressional committees on such prioritization and use.

(c) AGENCY RESPONSIBILITIES.—

(1) IN GENERAL.—Except as provided in paragraph (2)—

(A) not later than 1 year after the date of enactment of this Act or 2 months after the date on which the Secretary makes available the intrusion detection and prevention capabilities under section 230(b)(1) of the Homeland Security Act of 2002, as added by subsection (a), whichever is later, the head of each agency shall apply and continue to utilize the capabilities to all information traveling between an agency information system and any information system other than an agency information system; and

(B) not later than 6 months after the date on which the Secretary makes available improvements to the intrusion detection and prevention capabilities pursuant to section 230(b)(2) of the Homeland Security Act of 2002, as added by subsection (a), the head of each agency shall apply and continue to utilize the improved intrusion detection and prevention capabilities.

(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(3) DEFINITION.—In this subsection only, the term ''agency information system'' means an information system owned or operated by an agency.

(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to limit an agency from applying the intrusion detection and prevention capabilities under section 230(b)(1) of the Homeland Security Act of 2002, as added by subsection (a), at the discretion of the head of the agency or as provided in relevant policies, directives, and guidelines.

(d) TABLE OF CONTENTS AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 note) is amended by striking the items relating to the first section designated as section 226, the second section designated as section 226 (relating to the national cybersecurity and communications integration center), section 227, and section 228 and inserting the following:

''Sec. 226. Cybersecurity recruitment and retention.

''Sec. 227. National cybersecurity and communications integration center.

''Sec. 228. Cybersecurity plans.
''Sec. 229. Clearances.
''Sec. 230. Federal intrusion detection and prevention system.''.

SEC. 204. ADVANCED INTERNAL DEFENSES.

(a) ADVANCED NETWORK SECURITY TOOLS.—

(1) IN GENERAL.—The Secretary shall include in the Continuous Diagnostics and Mitigation Program advanced network security tools to improve visibility of network activity, including through the use of commercial and free or open source tools, to detect and mitigate intrusions and anomalous activity.

(2) DEVELOPMENT OF PLAN.—The Director shall develop and implement a plan to ensure that each agency utilizes advanced network security tools, including those described in paragraph (1), to detect and mitigate intrusions and anomalous activity.

(b) IMPROVED METRICS.—The Secretary, in collaboration with the Director, shall review and update the metrics used to measure security under section 3554 of title 44, United States Code, to include measures of intrusion and incident detection and response times.

(c) TRANSPARENCY AND ACCOUNTABILITY.—The Director, in consultation with the Secretary, shall increase transparency to the public on agency cybersecurity posture, including by increasing the number of metrics available on Federal Government performance websites and, to the greatest extent practicable, displaying metrics for department components, small agencies, and micro agencies.

(d) MAINTENANCE OF TECHNOLOGIES.—Section 3553(b)(6)(B) of title 44, United States Code, is amended by inserting '', operating, and maintaining'' after ''deploying''.

(e) EXCEPTION.—The requirements under this section shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

SEC. 205. FEDERAL CYBERSECURITY REQUIREMENTS.

(a) IMPLEMENTATION OF FEDERAL CYBERSECURITY STANDARDS.—Consistent with section 3553 of title 44, United States Code, the Secretary, in consultation with the Director, shall exercise the authority to issue binding operational directives to assist the Director in ensuring timely agency adoption of and compliance with policies and standards promulgated under section 11331 of title 40, United States Code, for securing agency information systems.

(b) CYBERSECURITY REQUIREMENTS AT AGENCIES.—

(1) IN GENERAL.—Consistent with policies, standards, guidelines, and directives on information security under subchapter II of chapter 35 of title 44, United States Code, and the standards and guidelines promulgated under section 11331 of title 40, United States Code, and except as provided in paragraph (2), not later than 1 year after the date of the enactment of this Act, the head of each agency shall—

(A) identify sensitive and mission critical data stored by the agency consistent with the inventory required under the first subsection (c) (relating to the inventory of major information systems) and the second subsection (c) (relating to the inventory of information systems) of section 3505 of title 44, United States Code;

(B) assess access controls to the data described in subparagraph (A), the need for readily accessible storage of the data, and individuals' need to access the data;

(C) encrypt or otherwise render indecipherable to unauthorized users the data described in subparagraph (A) that is stored on or transiting agency information systems;

(D) implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication, as developed by the Administrator of General Services in collaboration with the Secretary; and

(E) implement identity management consistent with section 504 of the Cybersecurity Enhancement Act of 2014 (Public Law 113–274; 15 U.S.C. 7464), including multi-factor authentication, for—

(i) remote access to an agency information system; and

(ii) each user account with elevated privileges on an agency information system.

(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to an agency information system for which—

(A) the head of the agency has personally certified to the Director with particularity that—

(i) operational requirements articulated in the certification and related to the agency information system would make it excessively burdensome to implement the cybersecurity requirement;

(ii) the cybersecurity requirement is not necessary to secure the agency information system or agency information stored on or transiting it; and

(iii) the agency has taken all necessary steps to secure the agency information system and agency information stored on or transiting it; and

(B) the head of the agency or the designee of the head of the agency has submitted the certification described in subparagraph (A) to the appropriate congressional committees and the agency's authorizing committees.

(3) CONSTRUCTION.—Nothing in this section shall be construed to alter the authority of the Secretary, the Director, or the Director of the National Institute of Standards and Technology in implementing subchapter II of chapter 35 of title 44, United States Code. Nothing in this section shall be construed to affect the National Institute of Standards and Technology standards process or the requirement under section 3553(a)(4) of such title or to discourage continued improvements and advancements in the technology, standards, policies, and guidelines used to promote Federal information security.

(c) EXCEPTION.—The requirements under this section shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

SEC. 206. ASSESSMENT; REPORTS.

(a) DEFINITIONS.—In this section—

(1) the term ''intrusion assessments'' means actions taken under the intrusion assessment plan to identify and remove intruders in agency information systems;

(2) the term ''intrusion assessment plan'' means the plan required under section 228(b)(1) of the Homeland Security Act of 2002, as added by section 203(a) of this Act; and

(3) the term ''intrusion detection and prevention capabilities'' means the capabilities required under section 230(b) of the Homeland Security Act of 2002, as added by section 203(a) of this Act.

(b) THIRD PARTY ASSESSMENT.—Not later than 3 years after the date of enactment of this Act, the Government Accountability Office shall conduct a study and publish a report on the effectiveness of the approach and strategy of the Federal Government to securing agency information systems, including the intrusion detection and prevention capabilities and the intrusion assessment plan.

(c) REPORTS TO CONGRESS.—

(1) INTRUSION DETECTION AND PREVENTION CAPABILITIES.—

(A) SECRETARY OF HOMELAND SECURITY REPORT.—Not later than 6 months after the date of enactment of this Act, and annually thereafter, the Secretary shall submit to the appropriate congressional committees a report on the status of implementation of the intrusion detection and prevention capabilities, including—

(i) a description of privacy controls;

(ii) a description of the technologies and capabilities utilized to detect cybersecurity risks in network traffic, including the extent to which those technologies and capabilities include existing commercial and non-commercial technologies;

(iii) a description of the technologies and capabilities utilized to prevent network traffic associated with cybersecurity risks from transiting or traveling to or from agency information systems, including the extent to which those technologies and capabilities include existing commercial and non-commercial technologies;

(iv) a list of the types of indicators or other identifiers or techniques used to detect cybersecurity risks in network traffic transiting or traveling to or from agency information systems on each iteration of the intrusion detection and prevention capabilities and the number of each such type of indicator, identifier, and technique;

(v) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from agency information systems and the number of times the intrusion detection and prevention capabilities blocked network traffic associated with cybersecurity risk; and

(vi) a description of the pilot established under section 230(c)(5) of the Homeland Security Act of 2002, as added by section 203(a) of this Act, including the number of new technologies tested and the number of participating agencies.

(B) OMB REPORT.—Not later than 18 months after the date of enactment of this Act, and annually thereafter, the Director shall submit to Congress, as part of the report required under section 3553(c) of title 44, United States Code, an analysis of agency application of the intrusion detection and prevention capabilities, including—

(i) a list of each agency and the degree to which each agency has applied the intrusion detection and prevention capabilities to an agency information system; and

(ii) a list by agency of—

(I) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such cybersecurity risks; and

(II) the number of instances in which the intrusion detection and prevention capabilities prevented network traffic associated with a cybersecurity risk from transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such agency information systems.

(2) OMB REPORT ON DEVELOPMENT AND IMPLEMENTATION OF INTRUSION ASSESSMENT PLAN, ADVANCED INTERNAL DEFENSES, AND FEDERAL CYBERSECURITY BEST PRACTICES.—The Director shall—

(A) not later than 6 months after the date of enactment of this Act, and 30 days after any update thereto, submit the intrusion assessment plan to the appropriate congressional committees;

(B) not later than 1 year after the date of enactment of this Act, and annually thereafter, submit to Congress, as part of the report required under section 3553(c) of title 44, United States Code—

(i) a description of the implementation of the intrusion assessment plan;

(ii) the findings of the intrusion assessments conducted pursuant to the intrusion assessment plan;

(iii) advanced network security tools included in the Continuous Diagnostics and Mitigation Program pursuant to section 204(a)(1);

(iv) the results of the assessment of the Secretary of best practices for Federal cybersecurity pursuant to section 205(a); and

(v) a list by agency of compliance with the requirements of section 205(b); and

(C) not later than 1 year after the date of enactment of this Act, submit to the appropriate congressional committees—

(i) a copy of the plan developed pursuant to section 204(a)(2); and

(ii) the improved metrics developed pursuant to section 204(b).

SEC. 207. TERMINATION.

(a) IN GENERAL.—The authority provided under section 230 of the Homeland Security Act of 2002, as added by section 203(a) of this Act, and the reporting requirements under section 206(c) shall terminate on the date that is 7 years after the date of enactment of this Act.

(b) RULE OF CONSTRUCTION.—Nothing in subsection (a) shall be construed to affect the limitation of liability of a private entity for assistance provided to the Secretary under section 230(d)(2) of the Homeland Security Act of 2002, as added by section 203(a) of this Act, if such assistance was rendered before the termination date under subsection (a) or otherwise during a period in which the assistance was authorized.

SEC. 208. IDENTIFICATION OF INFORMATION SYSTEMS RELATING TO NATIONAL SECURITY.

(a) IN GENERAL.—Except as provided in subsection (c), not later than 180 days after the date of enactment of this Act—

(1) the Director of National Intelligence and the Director of the Office of Management and Budget, in coordination with the heads of other agencies, shall—

(A) identify all unclassified information systems that provide access to information that may provide an adversary with the ability to derive information that would otherwise be considered classified;

(B) assess the risks that would result from the breach of each unclassified information system identified in subparagraph (A); and

(C) assess the cost and impact on the mission carried out by each agency that owns an unclassified information system identified in subparagraph (A) if the system were to be subsequently designated as a national security system; and

(2) the Director of National Intelligence and the Director of the Office of Management and Budget shall submit to the appropriate congressional committees, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives a report that includes the findings under paragraph (1).

(b) FORM.—The report submitted under subsection (a)(2) shall be in unclassified form, and shall include a classified annex.

(c) EXCEPTION.—The requirements under subsection (a)(1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to designate an information system as a national security system.

SEC. 209. DIRECTION TO AGENCIES.

(a) IN GENERAL.—Section 3553 of title 44, United States Code, is amended by adding at the end the following:

''(h) DIRECTION TO AGENCIES.—

''(1) AUTHORITY.—

''(A) IN GENERAL.—Subject to subparagraph (B), in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, the Secretary may issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat.

''(B) EXCEPTION.—The authorities of the Secretary under this subsection shall not apply to a system described subsection (d) or to a system described in paragraph (2) or (3) of subsection (e).

''(2) PROCEDURES FOR USE OF AUTHORITY.—The Secretary shall—

''(A) in coordination with the Director, establish procedures governing the circumstances under which a directive may be issued under this subsection, which shall include—

''(i) thresholds and other criteria;

''(ii) privacy and civil liberties protections; and

''(iii) providing notice to potentially affected third parties;

''(B) specify the reasons for the required action and the duration of the directive;

''(C) minimize the impact of a directive under this subsection by—

''(i) adopting the least intrusive means possible under the circumstances to secure the agency information systems; and

''(ii) limiting directives to the shortest period practicable;

''(D) notify the Director and the head of any affected agency immediately upon the issuance of a directive under this subsection;

''(E) consult with the Director of the National Institute of Standards and Technology regarding any directive under this subsection that implements standards and guidelines developed by the National Institute of Standards and Technology;

''(F) ensure that directives issued under this subsection do not conflict with the standards and guidelines issued under section 11331 of title 40;

''(G) consider any applicable standards or guidelines developed by the National Institute of Standards and issued by the Secretary of Commerce under section 11331 of title 40; and

''(H) not later than February 1 of each year, submit to the appropriate congressional committees a report regarding the specific actions the Secretary has taken pursuant to paragraph (1)(A).

''(3) IMMINENT THREATS.—

''(A) IN GENERAL.—Notwithstanding section 3554, the Secretary may authorize the intrusion detection and prevention capabilities under section 230(b)(1) of the Homeland Security Act of 2002 for the purpose of ensuring the security of agency information systems, if—

''(i) the Secretary determines there is an imminent threat to agency information systems;

''(ii) the Secretary determines a directive under subsection (b)(2)(C) or paragraph (1)(A) is not reasonably likely to result in a timely response to the threat;

''(iii) the Secretary determines the risk posed by the imminent threat outweighs any adverse consequences reasonably expected to result from the use of protective capabilities under the control of the Secretary;

''(iv) the Secretary provides prior notice to the Director, and the head and chief information officer (or equivalent official) of each agency to which specific actions will be taken pursuant to subparagraph (A), and notifies the appropriate congressional committees and authorizing committees of each such agencies within seven days of taking an action under this subsection of—

''(I) any action taken under this subsection; and

''(II) the reasons for and duration and nature of the action;

''(v) the action of the Secretary is consistent with applicable law; and

''(vi) the Secretary authorizes the use of protective capabilities in accordance with the advance procedures established under subparagraph (C).

''(B) LIMITATION ON DELEGATION.—The authority under this subsection may not be delegated by the Secretary.

''(C) ADVANCE PROCEDURES.—The Secretary shall, in coordination with the Director, and in consultation with the heads of Federal agencies, establish procedures governing the circumstances under which the Secretary may authorize the use of protective capabilities subparagraph (A). The Secretary shall submit the procedures to Congress.

''(4) LIMITATION.—The Secretary may direct or authorize lawful action or protective capability under this subsection only to—

''(A) protect agency information from unauthorized access, use, disclosure, disruption, modification, or destruction; or

''(B) require the remediation of or protect against identified information security risks with respect to—

''(i) information collected or maintained by or on behalf of an agency; or

''(ii) that portion of an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

''(i) ANNUAL REPORT TO CONGRESS.—Not later than February 1 of each year, the Director shall submit to the appropriate congressional committees a report regarding the specific actions the Director has taken pursuant to subsection (a)(5), including any actions taken pursuant to section 11303(b)(5) of title 40.

''(j) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term 'appropriate congressional committees' means—

''(1) the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate; and

''(2) the Committee on Appropriations, the Committee on Homeland Security, the Committee on Oversight and Government Reform, and the Committee on Science, Space, and Technology of the House of Representatives.''.

(b) CONFORMING AMENDMENT.—Section 3554(a)(1)(B) of title 44, United States Code, is amended—

(1) in clause (iii), by striking ''and'' at the end; and

(2) by adding at the end the following:

''(v) emergency directives issued by the Secretary under section 3553(h); and''.

TITLE III—FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT

SEC. 301. SHORT TITLE.

This title may be cited as the ''Federal Cybersecurity Workforce Assessment Act of 2015''.

SEC. 302. DEFINITIONS.

In this title:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Armed Services of the Senate;

(B) the Committee on Homeland Security and Governmental Affairs of the Senate;

(C) the Select Committee on Intelligence of the Senate;

(D) the Committee on Commerce, Science, and Transportation of the Senate;

(E) the Committee on Armed Services in the House of Representatives;

(F) the Committee on Homeland Security of the House of Representatives;

(G) the Committee on Oversight and Government Reform of the House of Representatives; and

(H) the Permanent Select Committee on Intelligence of the House of Representatives.

(2) DIRECTOR.—The term ''Director'' means the Director of the Office of Personnel Management.

(3) ROLES.—The term ''roles'' has the meaning given the term in the National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework.

SEC. 303. NATIONAL CYBERSECURITY WORKFORCE MEASUREMENT INITIATIVE.

(a) IN GENERAL.—The head of each Federal agency shall—

(1) identify all positions within the agency that require the performance of cybersecurity or other cyber-related functions; and

(2) assign the corresponding employment code, which shall be added to the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework, in accordance with subsection (b).

(b) EMPLOYMENT CODES.—

(1) PROCEDURES.—

(A) CODING STRUCTURE.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Commerce, acting through the National Institute of Standards and Technology, shall update the National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework to include a corresponding coding structure.

(B) IDENTIFICATION OF CIVILIAN CYBER PERSONNEL.—Not later than 9 months after the date of enactment of this Act, the Director, in coordination with the Director of the National Institute of Standards and Technology and the Director of National Intelligence, shall establish procedures to implement the National Initiative for Cybersecurity Education's coding structure to identify all Federal civilian positions that require the performance of information technology, cybersecurity, or other cyber-related functions.

(C) IDENTIFICATION OF NONCIVILIAN CYBER PERSONNEL.—Not later than 18 months after the date of enactment of this Act, the Secretary of Defense shall establish procedures to implement the National Initiative for Cybersecurity Education's coding structure to identify all Federal noncivilian positions that require the performance of information technology, cybersecurity, or other cyber-related functions.

(D) BASELINE ASSESSMENT OF EXISTING CYBERSECURITY WORKFORCE.—Not later than 3 months after the date on which the procedures are developed under subparagraphs (B) and (C), respectively, the head of each Federal agency shall submit to the appropriate congressional committees of jurisdiction a report that identifies—

(i) the percentage of personnel with information technology, cybersecurity, or other cyber-related job functions who currently hold the appropriate industry-recognized certifications as identified in the National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework;

(ii) the level of preparedness of other civilian and noncivilian cyber personnel without existing credentials to take certification exams; and

(iii) a strategy for mitigating any gaps identified in clause (i) or (ii) with the appropriate training and certification for existing personnel.

(E) PROCEDURES FOR ASSIGNING CODES.—Not later than 3 months after the date on which the procedures are developed under subparagraphs (B) and (C), respectively, the head of each Federal agency shall establish procedures—

(i) to identify all encumbered and vacant positions with information technology, cybersecurity, or other cyber-related functions (as defined in the National Initiative for Cybersecurity Education's coding structure); and

(ii) to assign the appropriate employment code to each such position, using agreed standards and definitions.

(2) CODE ASSIGNMENTS.—Not later than 1 year after the date after the procedures are established under paragraph (1)(E), the head of each Federal agency shall complete assignment of the appropriate employment code to each position within the agency with information technology, cybersecurity, or other cyber-related functions.

(c) PROGRESS REPORT.—Not later than 180 days after the date of enactment of this Act, the Director shall submit a progress report on the implementation of this section to the appropriate congressional committees.

SEC. 304. IDENTIFICATION OF CYBER-RELATED ROLES OF CRITICAL NEED.

(a) IN GENERAL.—Beginning not later than 1 year after the date on which the employment codes are assigned to employees pursuant to section 203(b)(2), and annually through 2022, the head of each Federal agency, in consultation with the Director, the Director of the National Institute of Standards and Technology, and the Secretary of Homeland Security, shall—

(1) identify information technology, cybersecurity, or other cyber-related roles of critical need in the agency's workforce; and

(2) submit a report to the Director that—

(A) describes the information technology, cybersecurity, or other cyber-related roles identified under paragraph (1); and

(B) substantiates the critical need designations.

(b) GUIDANCE.—The Director shall provide Federal agencies with timely guidance for identifying information technology, cybersecurity, or other cyber-related roles of critical need, including—

(1) current information technology, cybersecurity, and other cyber-related roles with acute skill shortages; and

(2) information technology, cybersecurity, or other cyber-related roles with emerging skill shortages.

(c) CYBERSECURITY NEEDS REPORT.—Not later than 2 years after the date of the enactment of this Act, the Director, in consultation with the Secretary of Homeland Security, shall—

(1) identify critical needs for information technology, cybersecurity, or other cyber-related workforce across all Federal agencies; and

(2) submit a progress report on the implementation of this section to the appropriate congressional committees.

SEC. 305. GOVERNMENT ACCOUNTABILITY OFFICE STATUS REPORTS.

The Comptroller General of the United States shall—

(1) analyze and monitor the implementation of sections 303 and 304; and

(2) not later than 3 years after the date of the enactment of this Act, submit a report to the appropriate congressional committees that describes the status of such implementation.

TITLE IV—OTHER CYBER MATTERS

SEC. 401. STUDY ON MOBILE DEVICE SECURITY.

(a) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Secretary of Homeland Security, in consultation with the Director of the National Institute of Standards and Technology, shall—

(1) complete a study on threats relating to the security of the mobile devices of the Federal Government; and

(2) submit an unclassified report to Congress, with a classified annex if necessary, that contains the findings of such study, the recommendations developed under paragraph (3) of subsection (b), the deficiencies, if any, identified under (4) of such subsection, and the plan developed under paragraph (5) of such subsection.

(b) MATTERS STUDIED.—In carrying out the study under subsection (a)(1), the Secretary, in consultation with the Director of the National Institute of Standards and Technology, shall—

(1) assess the evolution of mobile security techniques from a desktop-centric approach, and whether such techniques are adequate to meet current mobile security challenges;

(2) assess the effect such threats may have on the cybersecurity of the information systems and networks of the Federal Government (except for national security systems or the information systems and networks of the Department of Defense and the intelligence community);

(3) develop recommendations for addressing such threats based on industry standards and best practices;

(4) identify any deficiencies in the current authorities of the Secretary that may inhibit the ability of the Secretary to address mobile device security throughout the Federal Government (except for national security systems and the information systems and networks of the Department of Defense and intelligence community); and

(5) develop a plan for accelerated adoption of secure mobile device technology by the Department of Homeland Security.

(c) INTELLIGENCE COMMUNITY DEFINED.—In this section, the term ''intelligence community'' has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

SEC. 402. DEPARTMENT OF STATE INTERNATIONAL CYBERSPACE POLICY STRATEGY.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of State shall produce a comprehensive strategy relating to United States international policy with regard to cyberspace.

(b) ELEMENTS.—The strategy required by subsection (a) shall include the following:

(1) A review of actions and activities undertaken by the Secretary of State to date to support the goal of the President's International Strategy for Cyberspace, released in May 2011, to ''work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation.''.

(2) A plan of action to guide the diplomacy of the Secretary of State, with regard to foreign countries, including conducting bilateral and multilateral activities to develop the norms of responsible international behavior in cyberspace, and status review of existing discussions in multilateral fora to obtain agreements on international norms in cyberspace.

(3) A review of the alternative concepts with regard to international norms in cyberspace offered by foreign countries that are prominent actors, including China, Russia, Brazil, and India.

(4) A detailed description of threats to United States national security in cyberspace from foreign countries, state-sponsored actors, and private actors to Federal and private sector infrastructure of the United States, intellectual property in the United States, and the privacy of citizens of the United States.

(5) A review of policy tools available to the President to deter foreign countries, state-sponsored actors, and private actors, including those outlined in Executive Order 13694, released on April 1, 2015.

(6) A review of resources required by the Secretary, including the Office of the Coordinator for Cyber Issues, to conduct activities to build responsible norms of international cyber behavior.

(c) CONSULTATION.—In preparing the strategy required by subsection (a), the Secretary of State shall consult, as appropriate, with other agencies and departments of the United States and the private sector and nongovernmental organizations in the United States with recognized credentials and expertise in foreign policy, national security, and cybersecurity.

(d) FORM OF STRATEGY.—The strategy required by subsection (a) shall be in unclassified form, but may include a classified annex.

(e) AVAILABILITY OF INFORMATION.—The Secretary of State shall—

(1) make the strategy required in subsection (a) available the public; and

(2) brief the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives on the strategy, including any material contained in a classified annex.

SEC. 403. APPREHENSION AND PROSECUTION OF INTERNATIONAL CYBER CRIMINALS.

(a) INTERNATIONAL CYBER CRIMINAL DEFINED.—In this section, the term ''international cyber criminal'' means an individual—

(1) who is believed to have committed a cybercrime or intellectual property crime against the interests of the United States or the citizens of the United States; and

(2) for whom—

(A) an arrest warrant has been issued by a judge in the United States; or

(B) an international wanted notice (commonly referred to as a ''Red Notice'') has been circulated by Interpol.

(b) CONSULTATIONS FOR NONCOOPERATION.—The Secretary of State, or designee, shall consult with the appropriate government official of each country from which extradition is not likely due to the lack of an extradition treaty with the United States or other reasons, in which one or more international cyber criminals are physically present, to determine what actions the government of such country has taken—

(1) to apprehend and prosecute such criminals; and

(2) to prevent such criminals from carrying out cybercrimes or intellectual property crimes against the interests of the United States or its citizens.

(c) ANNUAL REPORT.—

(1) IN GENERAL.—The Secretary of State shall submit to the appropriate congressional committees an annual report that includes—

(A) the number of international cyber criminals located in other countries, disaggregated by country, and indicating from which countries extradition is not likely due to the lack of an extradition treaty with the United States or other reasons;

(B) the nature and number of significant discussions by an official of the Department of State on ways to thwart or prosecute international cyber criminals with an official of another country, including the name of each such country; and

(C) for each international cyber criminal who was extradited to the United States during the most recently completed calendar year—

(i) his or her name;

(ii) the crimes for which he or she was charged;

(iii) his or her previous country of residence; and

(iv) the country from which he or she was extradited into the United States.

(2) FORM.—The report required by this subsection shall be in unclassified form to the maximum extent possible, but may include a classified annex.

(3) APPROPRIATE CONGRESSIONAL COMMITTEES.—For purposes of this subsection, the term ''appropriate congressional committees'' means—

(A) the Committee on Foreign Relations, the Committee on Appropriations, the Committee on Homeland Security and Governmental Affairs, the Committee on Banking, Housing, and Urban Affairs, the Select Committee on Intelligence, and the Committee on the Judiciary of the Senate; and

(B) the Committee on Foreign Affairs, the Committee on Appropriations, the Committee on Homeland Security, the Committee on Financial Services, the Permanent Select Committee on Intelligence, and the Committee on the Judiciary of the House of Representatives.

SEC. 404. ENHANCEMENT OF EMERGENCY SERVICES.

(a) COLLECTION OF DATA.—Not later than 90 days after the date of enactment of this Act, the Secretary of Homeland Security, acting through the National Cybersecurity and Communications Integration Center, in coordination with appropriate Federal entities and the Director for Emergency Communications, shall establish a process by which a Statewide Interoperability Coordinator may report data on any cybersecurity risk or incident involving any information system or network used by emergency response providers (as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101)) within the State.

(b) ANALYSIS OF DATA.—Not later than 1 year after the date of enactment of this Act, the Secretary of Homeland Security, acting through the Director of the National Cybersecurity and Communications Integration Center, in coordination with appropriate entities and the Director for Emergency Communications, and in consultation with the Director of the National Institute of Standards and Technology, shall conduct integration and analysis of the data reported under subsection (a) to develop information and recommendations on security and resilience measures for any information system or network used by State emergency response providers.

(c) BEST PRACTICES.—

(1) IN GENERAL.—Using the results of the integration and analysis conducted under subsection (b), and any other relevant information, the Director of the National Institute of Standards and Technology shall, on an ongoing basis, facilitate and support the development of methods for reducing cybersecurity risks to emergency response providers using the process described in section 2(e) of the National Institute of Standards and Technology Act (15 U.S.C. 272(e)).

(2) REPORT.—The Director of the National Institute of Standards and Technology shall submit a report to Congress on the methods developed under paragraph (1) and shall make such report publically available on the website of the National Institute of Standards and Technology.

(d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to—

(1) require a State to report data under subsection (a); or

(2) require an entity to—

(A) adopt a recommended measure developed under subsection (b); or

(B) follow the best practices developed under subsection (c).

SEC. 405. IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY.

(a) DEFINITIONS.—In this section:

(1) BUSINESS ASSOCIATE.—The term ''business associate'' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(2) COVERED ENTITY.—The term ''covered entity'' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(3) HEALTH CARE CLEARINGHOUSE; HEALTH CARE PROVIDER; HEALTH PLAN.—The terms ''health care clearinghouse'', ''health care provider'', and ''health plan'' have the meanings given the terms in section 160.103 of title 45, Code of Federal Regulations.

(4) HEALTH CARE INDUSTRY STAKEHOLDER.—The term ''health care industry stakeholder'' means any—

(A) health plan, health care clearinghouse, or health care provider;

(B) patient advocate;

(C) pharmacist;

(D) developer of health information technology;

(E) laboratory;

(F) pharmaceutical or medical device manufacturer; or

(G) additional stakeholder the Secretary determines necessary for purposes of subsection (d)(1), (d)(3), or (e).

(5) SECRETARY.—The term ''Secretary'' means the Secretary of Health and Human Services.

(b) REPORT.—Not later than 1 year after the date of enactment of this Act, the Secretary shall submit, to the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Energy and Commerce of the House of Representatives, a report on the preparedness of the health care industry in responding to cybersecurity threats.

(c) CONTENTS OF REPORT.—With respect to the internal response of the Department of Health and Human Services to emerging cybersecurity threats, the report shall include—

(1) a clear statement of the official within the Department of Health and Human Services to be responsible for leading and coordinating efforts of the Department regarding cybersecurity threats in the health care industry; and

(2) a plan from each relevant operating division and subdivision of the Department of Health and Human Services on how such division or subdivision will address cybersecurity threats in the health care industry, including a clear delineation of how each such division or subdivision will divide responsibility among the personnel of such division or subdivision and communicate with other such divisions and subdivisions regarding efforts to address such threats.

(d) HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE.—

(1) IN GENERAL.—Not later than 60 days after the date of enactment of this Act, the Secretary, in consultation with the Director of the National Institute of Standards and Technology and the Secretary of Homeland Security, shall convene health care industry stakeholders, cybersecurity experts, and any Federal agencies or entities the Secretary determines appropriate to establish a task force to—

(A) analyze how industries, other than the health care industry, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries;

(B) analyze challenges and barriers private entities (notwithstanding section 102(15)(B), excluding any State, tribal, or local government) in the health care industry face securing themselves against cyber attacks;

(C) review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record;

(D) provide the Secretary with information to disseminate to health care industry stakeholders for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the health care industry;

(E) establish a plan for creating a single system for the Federal Government to share information on actionable intelligence regarding cybersecurity threats to the health care industry in near real time, requiring no fee to the recipients of such information, including which Federal agency or other entity may be best suited to be the central conduit to facilitate the sharing of such information; and

(F) report to Congress on the findings and recommendations of the task force regarding carrying out subparagraphs (A) through (E).

(2) TERMINATION.—The task force established under this subsection shall terminate on the date that is 1 year after the date of enactment of this Act.

(3) DISSEMINATION.—Not later than 60 days after the termination of the task force established under this subsection, the Secretary shall disseminate the information described in paragraph (1)(D) to health care industry stakeholders in accordance with such paragraph.

(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to limit the antitrust exemption under section 104(e) or the protection from liability under section 106.

(e) CYBERSECURITY FRAMEWORK.—

(1) IN GENERAL.—The Secretary shall establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, the National Institute of Standards and Technology, and any Federal agency or entity the Secretary determines appropriate, a single, voluntary, national health-specific cybersecurity framework that—

(A) establishes a common set of voluntary, consensus-based, and industry-led standards, security practices, guidelines, methodologies, procedures, and processes that serve as a resource for cost-effectively reducing cybersecurity risks for a range of health care organizations;

(B) supports voluntary adoption and implementation efforts to improve safeguards to address cybersecurity threats;

(C) is consistent with the security and privacy regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note) and with the Health Information Technology for Economic and Clinical Health Act (title XIII of division A, and title IV of division B, of Public Law 111–5), and the amendments made by such Act; and

(D) is updated on a regular basis and applicable to the range of health care organizations described in subparagraph (A).

(2) LIMITATION.—Nothing in this subsection shall be interpreted as granting the Secretary authority to—

(A) provide for audits to ensure that health care organizations are in compliance with the voluntary framework under this subsection; or

(B) mandate, direct, or condition the award of any Federal grant, contract, or purchase on compliance with such voluntary framework.

(3) NO LIABILITY FOR NONPARTICIPATION.—Nothing in this title shall be construed to subject a health care organization to liability for choosing not to engage in the voluntary activities authorized under this subsection.

SEC. 406. FEDERAL COMPUTER SECURITY.

(a) DEFINITIONS.—In this section:

(1) COVERED SYSTEM.—The term ''covered system'' shall mean a national security system as defined in section 11103 of title 40, United States Code, or a Federal computer system that provides access to personally identifiable information.

(2) COVERED AGENCY.—The term ''covered agency'' means an agency that operates a covered system.

(3) LOGICAL ACCESS CONTROL.—The term ''logical access control'' means a process of granting or denying specific requests to obtain and use information and related information processing services.

(4) MULTI-FACTOR LOGICAL ACCESS CONTROLS.—The term ''multi-factor logical access controls'' means a set of not less than 2 of the following logical access controls:

(A) Information that is known to the user, such as a password or personal identification number.

(B) An access device that is provided to the user, such as a cryptographic identification device or token.

(C) A unique biometric characteristic of the user.

(5) PRIVILEGED USER.—The term ''privileged user'' means a user who, by virtue of function or seniority, has been allocated powers within a covered system, which are significantly greater than those available to the majority of users.

(b) INSPECTOR GENERAL REPORTS ON COVERED SYSTEMS.—

(1) IN GENERAL.—Not later than 240 days after the date of enactment of this Act, the Inspector General of each covered agency shall submit to the appropriate committees of jurisdiction in the Senate and the House of Representatives a report, which shall include information collected from the covered agency for the contents described in paragraph (2) regarding the Federal computer systems of the covered agency.

(2) CONTENTS.—The report submitted by each Inspector General of a covered agency under paragraph (1) shall include, with respect to the covered agency, the following:

(A) A description of the logical access standards used by the covered agency to access a covered system, including—

(i) in aggregate, a list and description of logical access controls used to access such a covered system; and

(ii) whether the covered agency is using multi-factor logical access controls to access such a covered system.

(B) A description of the logical access controls used by the covered agency to govern access to covered systems by privileged users.

(C) If the covered agency does not use logical access controls or multi-factor logical access controls to access a covered system, a description of the reasons for not using such logical access controls or multi-factor logical access controls.

(D) A description of the following data security management practices used by the covered agency:

(i) The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.

(ii) What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including—

(I) data loss prevention capabilities; or

(II) digital rights management capabilities.

(iii) A description of how the covered agency is using the capabilities described in clause (ii).

(iv) If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.

(E) A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the data security management practices described in subparagraph (D).

(3) EXISTING REVIEW.—The reports required under this subsection may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the covered agency, and may be submitted as part of another report, including the report required under section 3555 of title 44, United States Code.

(4) CLASSIFIED INFORMATION.—Reports submitted under this subsection shall be in unclassified form, but may include a classified annex.

SEC. 407. STRATEGY TO PROTECT CRITICAL INFRASTRUCTURE AT GREATEST RISK.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE AGENCY.—The term ''appropriate agency'' means, with respect to a covered entity—

(A) except as provided in subparagraph (B), the applicable sector-specific agency; or

(B) in the case of a covered entity that is regulated by a Federal entity, such Federal entity.

(2) APPROPRIATE AGENCY HEAD.—The term ''appropriate agency head'' means, with respect to a covered entity, the head of the appropriate agency.

(3) COVERED ENTITY.—The term ''covered entity'' means an entity identified pursuant to section 9(a) of Executive Order 13636 of February 12, 2013 (78 Fed. Reg. 11742), relating to identification of critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

(4) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Select Committee on Intelligence of the Senate;

(B) the Permanent Select Committee on Intelligence of the House of Representatives;

(C) the Committee on Homeland Security and Governmental Affairs of the Senate;

(D) the Committee on Homeland Security of the House of Representatives;

(E) the Committee on Energy and Natural Resources of the Senate;

(F) the Committee on Energy and Commerce of the House of Representatives; and

(G) the Committee on Commerce, Science, and Transportation of the Senate.

(5) SECRETARY.—The term ''Secretary'' means the Secretary of the Department of Homeland Security.

(b) STATUS OF EXISTING CYBER INCIDENT REPORTING.—

(1) IN GENERAL.—No later than 120 days after the date of the enactment of this Act, the Secretary, in conjunction with the appropriate agency head (as the case may be), shall submit to the appropriate congressional committees describing the extent to which each covered entity reports significant intrusions of information systems essential to the operation of critical infrastructure to the Department of Homeland Security or the appropriate agency head in a timely manner.

(2) FORM.—The report submitted under paragraph (1) may include a classified annex.

(c) MITIGATION STRATEGY REQUIRED FOR CRITICAL INFRASTRUCTURE AT GREATEST RISK.—

(1) IN GENERAL.—No later than 180 days after the date of the enactment of this Act, the Secretary, in conjunction with the appropriate agency head (as the case may be), shall conduct an assessment and develop a strategy that addresses each of the covered entities, to ensure that, to the greatest extent feasible, a cyber security incident affecting such entity would no longer reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

(2) ELEMENTS.—The strategy submitted by the Secretary with respect to a covered entity shall include the following:

(A) An assessment of whether each entity should be required to report cyber security incidents.

(B) A description of any identified security gaps that must be addressed.

(C) Additional statutory authority necessary to reduce the likelihood that a cyber incident could cause catastrophic regional or national effects on public health or safety, economic security, or national security.

(3) SUBMITTAL.—The Secretary shall submit to the appropriate congressional committees the assessment and strategy required by paragraph (1).

(4) FORM.—The assessment and strategy submitted under paragraph (3) may each include a classified annex.

SEC. 408. STOPPING THE FRAUDULENT SALE OF FINANCIAL INFORMATION OF PEOPLE OF THE UNITED STATES.

Section 1029(h) of title 18, United States Code, is amended by striking ''title if—'' and all that follows through ''therefrom.'' and inserting ''title if the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity organized under the laws of the United States, or any State, the District of Columbia, or other Territory of the United States.''.

SEC. 409. 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.

The PRESIDING OFFICER. The majority leader.

MORNING BUSINESS

Mr. MCCONNELL. Madam President, I ask unanimous consent that the Senate be in a period of morning business, with Senators permitted to speak therein for up to 10 minutes each.

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

The Senator from Iowa.

NATIONAL DOMESTIC VIOLENCE AWARENESS MONTH

Mr. GRASSLEY. Madam President, I think we have clearance on a noncontroversial resolution that is going to pass yet this evening, and I rise for about 5 minutes to speak on this issue.

Last week I submitted a resolution to commemorate the goals and ideals of National Domestic Violence Awareness Month, which takes place each October. I thank Senators LEAHY, AYOTTE, and KLOBUCHAR for joining me as original cosponsors of this measure.

I have met with many domestic violence victims over the years. We have come a long way since the enactment in 1984, with my support, of the landmark Family Violence Prevention and Services Act.

In the decades since then, Congress has committed billions of dollars to implement that statute, as well as the Violence Against Women Act, and we have seen a decline in the rate of serious partner violence over the last two decades, according to the Congressional Research Service.

But researchers and advocates who work with domestic violence survivors remind us that there is still much work to be done to stop this terrible crime and support survivors in their efforts to heal. It is estimated that as many as 9 million Americans are physically abused by a partner every year.

According to a 2011 survey by the Centers for Disease Control and Prevention, about 22 percent of women and about 14 percent of men have experienced severe physical abuse by a partner in their lifetime.

Experts tell us that domestic violence affects women, men, and children of every age and socioeconomic class, but we also know that women still experience more domestic violence than do men, and women are significantly more likely to be injured in an assault by a partner or a spouse.

According to the Justice Department's Bureau of Justice Statistics, women between the ages of 18 and 31 experience the highest rates of domestic violence. Most have been victimized by the same offender on at least one prior occasion. And, of course, it is heartbreaking to realize that millions of American children have been exposed to domestic violence, either by experiencing some form of abuse or witnessing a family member's abuse.

The good news is that each and every day, in communities across the Nation, there are victim advocates, service providers, crisis hotline staff and volunteers, as well as first responders who are working tirelessly to extend compassionate service to the survivors of domestic violence. I wish to take this opportunity to single out some of these folks and extend a special thank-you on behalf of the Senate.

First, I highlight the hard work of trained volunteers and staff who operate crisis hotlines across the country. They are a varied and talented group of individuals who, often at low or no pay, make confidential support, information, and referrals available to victims, as well as their friends and families, each and every day. We appreciate their efforts to help countless men, women, and children escape abusive situations.

Next, I recognize the contributions of the talented staff at the 56 State and territorial domestic violence coalitions around the country and the globe. These individuals also help respond to the needs of battered men, women, and children, typically by offering their expertise and technical support to local domestic violence programs in each and every State and territory. In my home State, for example, the Iowa State Coalition Against Domestic Violence has, since way back in 1985, connected local service providers to vitally important training and other resources that exist to support Iowa survivors.

We cannot commemorate Domestic Violence Awareness Month without also mentioning the police officers who are on the front lines in the effort to protect crime victims and to prevent abuse in the first place. Domestic violence calls can present lethal risks for officers, and we mourn those who have lost their lives while responding to such domestic violence incidents. We know, too, that in recent decades the law enforcement approach to these instances has changed to reflect the latest research, and we applaud those police agencies that continue to update and improve their domestic violence policies.

I also recognize those who operate the Nation's domestic violence shelters that meet the emergency housing needs of thousands of adults and children each day or millions of Americans each year. Last but not least, I want to highlight the hard work of the staff at charities and agencies across the Nation that are devoted to helping domestic violence survivors achieve financial independence, obtain legal assistance, and most importantly overcome the detrimental emotional and physical effects of abuse.

As I close, I urge my colleagues to support the adoption of this important resolution. With its adoption, we demonstrate the Senate supports the goals and ideals of National Domestic Violence Awareness Month.

I yield the floor.

The PRESIDING OFFICER (Mr. PERDUE). The Senator from Rhode Island.

Mr. WHITEHOUSE. Mr. President, I ask unanimous consent to speak for up to 20 minutes in morning business.

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

CLIMATE CHANGE

Mr. WHITEHOUSE. Mr. President, there has been some activity on the Senate floor today regarding the President's Clean Power Plan, with fossil fuel State representatives coming to decry that plan. I would simply note that on October 22, in the Wall Street Journal, many of the leaders of America's national security took out an advertisement to say: ''Republicans & Democrats Agree: U.S. Security Demands Global Climate Action.''

We have had generals and admirals, former National Security Advisers and Directors of National Intelligence, Secretaries of the Treasury, Secretaries of Defense, Directors of the Central Intelligence Agency, Chairman of the National Intelligence Council, Governors, Senators, Under Secretaries of State, many Republicans all saying this is important; that it is time for America to lead. And what do we get? We get complaints about America leading.

If my friends have a better idea than the Clean Power Plan, I would be glad to listen. I am sure we would all be glad to listen. What is it? What is the other plan? Because if you have nothing, then you really don't have a seat at the table and you certainly don't have occasion to criticize what the President is trying to do. Show us something—anything. What have you got? Where is the Republican bill that even talks about climate change—let alone does anything serious about it.

It is truly time for this body to wake up and not just wake up to climate change but also to the decades-long purposeful corporate smokescreens of misleading statements from the fossil fuel industry and its allies on the dangers of carbon pollution. So I am here for the 116th time seeking an open, honest, and factual debate in Congress about global climate change.

The energy industry's top dog, ExxonMobil—No. 2 for both revenue and profits among the Fortune 500 of companies—has been getting some bad press lately. Two independent investigative reports from InsideClimate News and the Los Angeles Times revealed that Exxon's own scientists understood as far back as the late 1970s the effects of carbon pollution on the climate and warned company executives of the potential outcomes for the planet and humankind, but Exxon's own internal report also recognized heading off global warming ''would require major reductions in fossil fuel combustion.''

So what did this fossil fuel company do? Rather than behave responsibly, rather than face up to that truth, rather than lead an effort to stave off catastrophic emerging changes to the climate and the oceans, what Exxon chose to do was to fund and participate in a massive misinformation campaign to protect their business model and their bottom line.

This started right at the top. Exxon's former chairman and CEO Lee Raymond repeatedly and publicly questioned the science behind climate change, notwithstanding what his own scientists had said. ''Currently,'' Raymond claimed in a 1996 speech before the Economic Club of Detroit—20 years after this work by his own scientists—''the scientific evidence is inclusive as to whether human activities are having a significant effect on the global climate.''

There was already an emerging international consensus that unchecked carbon emissions were warming the planet. There was already Exxon's own internal research that showed carbon emissions were warming the planet, and it has gone forward to now with the latest report from the Intergovernmental Panel on Climate Change stating that ''warming of the climate system is unequivocal.'' Unequivocal.

The current ExxonMobil CEO, Rex Tillerson, still emphasizes uncertainty and goes out of his way to overestimate the costs of taking action. In 2013, he asked: ''What good is it to save the planet if humanity suffers?'' All right, someone needs to explain to me how if we fail to save the planet, humanity does not suffer. I guess it is Exxon's position that we only suffer if we try to save the planet.

At this year's annual shareholders meeting, Mr. Tillerson argued that the world needs to wait—that is always their argument, the world needs to wait—for the science to improve—unequivocal is evidently not enough—and to look for solutions to the effects of climate change as they become more clear—more clear.

Our oceans are clearly warming and acidifying, and this has been clearly measured. Atmospheric carbon is clearly higher than ever in our species' history on this planet, and this has been clearly measured. In Rhode Island, we have measured nearly 10 inches of sea level rise since the 1930s, right on our shores. What is not clear?

While Exxon was peddling climate denial here in Washington, the L.A. Times reports, they were using climate models to plan operations in the warming Arctic. Between 1986 and 1992, Exxon's senior ice researcher, Ken Croasdale, and others studied the effects global warming would have on Arctic oil operations and reported back to Exxon brass. They knew melting ice would lower exploration and development costs. They also knew higher seas and thawing permafrost would threaten the company's ships, drilling platforms, processing plants, and pipelines.

So Exxon was challenging the climate models publicly while it was using them privately to guide its own investment decisions. Exxon understood the dangers, but instead of sounding the alarm or trying to help, they chose to sow doubt.

Then there are the Exxon front groups. A study out just last month in the peer-reviewed journal Climatic Change says that ExxonMobil paid over $16 million between 1988 and 2005 to a network of phony-baloney think tanks and psuedoscience groups that spread misleading claims about climate science. The company's network includes organizations that name themselves after John Locke, James Madison, Benjamin Franklin, and even George C. Marshall. It also includes the American Legislative Exchange Council, or ALEC, which pedals anti-climate legislation in State legislatures. ALEC denies the human contribution to climate change by calling it a ''historical phenomenon,'' asserting ''the debate will continue on the significance of natural and anthropogenic contributions.'' The climate denial coming out of ALEC is so egregious even Shell Oil left the group this summer.

Don't forget the paid-for scientists. The Exxon network includes Willie Soon, whose work consistently downplayed the role of carbon pollution in climate change. Well, investigative reporting revealed Dr. Soon received more than $1.2 million from oil and coal interests, including ExxonMobil, over the last decade.

So the cat is out of the bag now, and all the bad press has got Exxon a little jumpy. Exxon's VP of Public Affairs, Ken Cohen, took to Exxon's blog to proclaim that his company has a legitimate history when it comes to climate. ''Our scientists have been involved in climate research and related policy analysis for more than 30 years, yielding more than 50 papers in peer-reviewed publications,'' he said. He goes on to say that Exxon has been involved with the U.N. IPCC, the National Academy of Science's National Climate Assessment, and that Exxon funds legitimate scientists at major universities as they research energy and climate.

Right. The problem is that is only half the story. That is the half of the story that shows Exxon knew better. What is the rest of the story? Decades of funding to a network of front groups that led a PR campaign designed to undercut climate science and prevent legitimate action on climate change. For decades, Exxon invested in legitimate climate research, you say? That is the proof of actual knowledge. That makes the route they chose of denial and delay all the more culpable, and that denial and delay, as Paul Harvey would say, is the rest of the story.

What are Tillerson and ExxonMobil waiting for? Why this campaign of deceit, denial, and delay? Sadly, it is our American system of big business and paid-for politics—just follow the money.

Exxon foists the costs of its carbon pollution on the rest of us—on our children, on our grandchildren—and all the while they make staggering amounts of money. And Congress, funded by their lobbyists, sleeps placidly at the switch.

Exxon even fights to protect their status quo with their own shareholders. The Institute for Policy Studies reports that shareholders of ExxonMobil have introduced 62 climate-related resolutions over the past 25 years, and all of them have been opposed by management. Rex Tillerson, who made $21.4 million in stock-based pay in 2014, has openly mocked a shareholder who asked about investing in renewables. This is rich. Tillerson responded that renewable energy ''only survives on the backs of enormous government mandates that are not sustainable. We on purpose choose not to lose money.''

Well, ExxonMobil spends huge amounts of money on the complex PR machine to churn out doubt about the real science in order to protect the

market subsidy that ignores the costs of Exxon's carbon pollution and makes clean energy face an uphill battle. So it is really kind of nervy to say that clean energy survives on the backs of enormous government subsidies when oil gets the biggest subsidies ever.

Things could have been different. Exxon could have heeded the warnings of its own scientists and helped us make a transition to clean energy. It is happening now without them. The International Energy Agency found that the cost of generating electricity from renewable sources dropped from $500 a megawatt hour in 2010 to $200 in 2015. Imagine if we had rolled up our sleeves and gotten to work way back when Exxon first learned of the dangers of carbon pollution. Imagine the leadership that company could have shown. Imagine how much of the coming climate and ocean changes we could have avoided. But they didn't, and the time of reckoning may now be upon the likes of Exxon and others in the fossil fuel industry. That PR machine may end up costing the company a lot. Look at what happened to big tobacco.

Two weeks ago, Congressmen TED LIEU and MARK DESAULNIER sent a letter to Attorney General Loretta Lynch regarding these newly reported allegations that ExxonMobil intentionally hid the truth about the role of fossil fuels in influencing climate change. ''The apparent tactics employed by Exxon are reminiscent of the actions employed by big tobacco companies to deceive the American people about the known risks of tobacco.''

Last week, my friend, the junior Senator from Vermont, joined in the call for the Attorney General to bring a civil RICO investigation into big fossil fuel. ''These reports, if true,'' reads Senator SANDERS' letter to Attorney General Lynch, ''raise serious allegations of a misinformation campaign that may have caused public harm similar to the tobacco industry's actions—conduct that led to federal racketeering convictions''—actually, a judgment. It was civil. But it is otherwise accurate.

Also last week, Sharon Eubanks, the former U.S. Department of Justice attorney who actually brought the civil action and won the civil RICO case against the tobacco industry, said that, considering recent revelations regarding ExxonMobil, the Department of Justice should consider launching an investigation into big fossil fuel companies—that it ''is plausible and should be considered.'' That was her quote.

Let me show why it is plausible and should be considered. Let me read from U.S. District Judge Gladys Kessler's description of the culpable conduct in her decision in the government's racketeering case against Big Tobacco:

Each and every one of these Defendants repeatedly, consistently, vigorously—and falsely—denied the existence of any adverse health effects from smoking. Moreover, they mounted a coordinated, well-financed, sophisticated public relations campaign to attack and distort the scientific evidence demonstrating the relationship between smoking and disease, claiming that the link between the two was still an ''open question.''

Defendants knew there was a consensus in the scientific community that smoking caused lung cancer and other diseases. Despite that fact, they publicly insisted that there was a scientific controversy and disputed scientific findings linking smoking and disease knowing their assertions were false.

Now, let's read that exact same language back but apply it to climate.

Each and every one of these Defendants repeatedly, consistently, vigorously—and falsely—denied the existence of any adverse [climate] effects from [carbon pollution]. Moreover, they mounted a coordinated, well-financed, sophisticated public relations campaign to attack and distort the scientific evidence demonstrating the relationship between [carbon pollution] and [climate], claiming that the link between the two was still an ''open question.''

Defendants knew there was a consensus in the scientific community that [carbon pollution] caused [climate change] and other [harms]. Despite that fact, they publicly insisted that there was a scientific controversy and disputed scientific findings linking [carbon pollution] and [climate] knowing their assertions were false.

Just change the words, and there is her judgment against the tobacco industry, and it plainly applies to climate denial.

The investigative journalism from InsideClimate News and the Los Angeles Times is damning. The calls for greater scrutiny of ExxonMobil and the fossil fuel industry are mounting, and the phony-baloney denial network is up in arms, trying to shovel this campaign under the protection of the First Amendment. Sorry, guys, the First Amendment doesn't protect fraud.

Describing Caesar at the Battle of Monda, Napoleon said: ''There is a moment in combat when the slightest maneuver is decisive and gives superiority; it is the drop of water that starts the overflow.''

Is the tide turning? Is this the decisive moment? Despite documented warnings from their own scientists dating from the 1970s, ExxonMobil and others pursued a campaign of deceit, denial, and delay. They may soon have to face the consequences. In any event, history will not look kindly on their choice.

I yield the floor.

The PRESIDING OFFICER. The Senator from Tennessee.

NO CHILD LEFT BEHIND REFORM

Mr. ALEXANDER. Mr. President, over the weekend President Obama announced that all 100,000 public schools across the Nation should limit testing to 2 percent of a student's time in the classroom. It is a recommendation, not a requirement, and it comes in response to a nationwide backlash from teachers, students, and parents who are sick of overtesting.

I was glad to see the President's comments. He is right about students taking too many tests. But I hope the President will stop and think before trying to cure overtesting by telling teachers exactly how much time to spend on testing or what the tests should be. Classroom teachers know better than Washington how to assess their students' progress. They also know that the real reason we have too many tests is that there are too many Federal mandates that put high stakes on student test results and that one more Washington decree—even if it is only a recommendation for now—is not the way to solve the problem of too many Federal mandates.

Instead, the best way to fix overtesting is to get rid of the Federal mandates that are causing the problem. That is precisely what the Senate did when it passed by an overwhelming bipartisan majority, 81 to 17, legislation to fix No Child Left Behind and give more flexibility to States and to classroom teachers to decide which tests will decide what progress students are making in the classroom.

No Child Left Behind, a Federal law enacted in 2001, requires students to take 17 standardized tests over the course of their education, kindergarten through the 12th grade. It then uses those tests to decide whether schools and teachers are succeeding or failing.

In the Senate's work to fix No Child Left Behind, no issue stirred as much controversy as these high-stakes tests. At first, I was among those who thought the best way to fix overtesting might be to get rid of the 17 Federal tests. But the more we studied the problem, the more the issues seemed not to be the 17 Federal tests but the federally designed system of rewarding and punishing schools and teachers that was attached to the tests.

A third grader, for example, is required to take only one test in math and one in reading. Each of those tests probably takes 1 or 2 hours, according to testimony before our committee. But here is the problem: The results of these tests count so much in the federally mandated accountability system that States and school districts are giving students dozens of additional tests to prepare for the Federal tests.

A new survey says students in big-city schools will take, on average, 112 mandatory standardized tests between prekindergarten and high school graduation. That is eight tests a year. One Florida study showed that a Fort Myers school district gave more than 160 tests to its students. Only 17 of those are federally required.

So after hearing this, the Senate decided to keep the federally required 17 tests. That is two annual tests in reading and math in grades 3 through 8 and once in high school, as well as science tests given three times between grades 3 and 12. We also kept the practice of reporting results publicly so parents and teachers know how their children are performing. These results are disaggregated, so we know how students are doing based upon their gender, their ethnicity or their disability.

Then, to discourage overtesting, we restored to States and classroom teachers the responsibility for deciding how to use these Federal test scores to measure achievement.

The Senate bill ends the high-stakes, Washington-designed, test-based accountability system that has caused the explosion of tests in our local schools. The Senate bill reverses the trend toward a national school board.

I am glad to see President Obama's focus on overtesting, but let's not make the same mistake twice by decreeing from Washington exactly how much time to spend on tests or what the tests should be. States and 3 million teachers in 100,000 public schools are in the best position to know what to do about overtesting our children.

Both the Senate and the House of Representatives have now passed similar bills to fix No Child Left Behind and to reduce the Federal mandates that are the real cause of overtesting. The best way to have fewer and better tests in America's classrooms is for Congress to finish its work and the President to sign our legislation before the end of the year.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

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

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

JAPANESE POW FRIENDSHIP PROGRAM

Mr. DURBIN. Mr. President, I would like to take a moment to call attention to a group of our Nation's veterans who participated in a reconciliation program with the Japanese Government.

From October 11 to October 19, nine veterans of the U.S. Army, U.S. Army Air Corps, and the U.S. Marines who fought bravely in the Pacific theater of World War II and were taken prisoner by Japanese forces traveled to Japan. They were guests of the Japanese Government on a trip of reconciliation and remembrance.

Established in 2010, this was the sixth Japanese POW Friendship Program delegation. This program is sponsored by the Japanese Ministry of Foreign Affairs for World War II POWs from the United States, with Japan running similar friendship programs with Australia and Britain.

More than 30,000 Allied troops were taken prisoner in Japan, many of them Americans who faced horrific ordeals. Today, 70 years following the end of World War II, this program reflects the journey of forgiveness and resolution between the United States and Japan, as our relationship has developed into one of the most critical in the region.

I would like to take a moment to acknowledge the veterans who were members of this year's delegation: Joseph DeMott, a U.S. Army Air Corps veteran from Litiz, PA; Arthur Gruenberg, a U.S. Marine Corps veteran from Camano Island, WA; George Hirschkamp, a U.S. Marine Corps veteran from Sandpoint, ID; George Rodgers, a U.S. Army veteran from Lynchburg, VA; Jack Warner, a U.S. Marine Corps veteran from Elk City, OK; and Clifford Warren, a U.S. Army veteran from Shepherd, TX.

I would also like to recognize three members of the delegation who are my constituents: Leland Chandler, a U.S. Army veteran from Galesburg, IL; William Chittenden, a U.S. Marine Corps veteran from Wheaton, IL; and Carl Dyer, a U.S. Army veteran from Oglesby, IL.

I am so grateful to all of these participants for their years of service to our Nation.

The delegation was accompanied by Jan Thompson, another Illinois constituent and a documentary filmmaker and daughter of a World War II veteran who was himself a POW in Japan. Thompson also heads the nonprofit veterans organization American Defenders of Bataan & Corregidor Memorial Society.

The Japanese POW Friendship Program and the American veterans who participate in it represent the transformation and strength of the U.S.-Japan relationship. I hope this program continues to bring together our two nations in remembrance and reconciliation.

BUDGETARY REVISIONS

Mr. ENZI. Mr. President, section 4380 of S. Con. Res. 11, the concurrent resolution on the budget for fiscal year 2016, allows the chairman of the Senate Budget Committee to revise the allocations, aggregates, and levels in the budget resolution for legislation that increases sharing of cyber security threat information while protecting individual privacy and civil liberties interests. The authority to adjust is contingent on the legislation not increasing the deficit over either the period of the total of fiscal years 2016–2020 or the period of the total of fiscal years 2016–2025.

I find that S. 754, as amended, fulfills the conditions of deficit neutrality found in section 4380 of S. Con. Res. 11. Accordingly, I am revising the allocation to the Select Committee on Intelligence and the budgetary aggregates to account for the budget effects of the amendment. As the budgetary effects of S. 754, as amended, are insignificant under our accounting methods, budgetary figures remain numerically unchanged.

BUDGET SCOREKEEPING REPORT

Mr. ENZI. Mr. President, I wish to submit to the Senate the budget scorekeeping report for October 2015. The report compares current law levels of spending and revenues with the amounts provided in the conference report to accompany S. Con. Res. 11, the budget resolution for fiscal year 2016. This information is necessary to determine whether budget points of order lie against pending legislation. It has been prepared by the Republican staff of the Senate Budget Committee and the Congressional Budget Office, CBO, pursuant to section 308(b) of the Congressional Budget Act.

This is the third report I have made since adoption of the fiscal year 2016 budget resolution on May 5, 2015. My last filing can be found in the CONGRESSIONAL RECORD on September 10, 2015. The information contained in this report is current through October 26, 2015.

Table 1 gives the amount by which each Senate authorizing committee is below or exceeds its allocation under the budget resolution. This information is used for enforcing committee allocations pursuant to section 302 of the Congressional Budget Act of 1974, CBA. For fiscal year 2015, which ended on September 30, 2015, Senate authorizing committees have increased direct spending outlays by $7.8 billion more than the agreed upon spending levels. Over the fiscal year 2016–2025 period, which is the entire period covered by S. Con. Res. 11, Senate authorizing committees have spent $2.2 billion less than the budget resolution calls for.

Table 2 gives the amount by which the Senate Committee on Appropriations is below or exceeds the statutory spending limits. This information is used to determine points of order related to the spending caps found in section 312 and section 314 of the CBA. While no full-year appropriations bills have been enacted for fiscal year 2016, subcommittees are charged with permanent and advanced appropriations that first become available in that year.

Table 3 gives the amount by which the Senate Committee on Appropriations is below or exceeds its allocation for overseas contingency operations/global war on terrorism, OCO/GWOT, spending. This separate allocation for OCO/GWOT was established in section 3102 of S. Con. Res. 11 and is enforced using section 302 of the CBA. No bills providing funds with the OCO/GWOT designation on a full-year basis have been enacted thus far for fiscal year 2016.

The budget resolution established two new points of order limiting the use of changes in mandatory programs in appropriations bills, CHIMPS. Tables 4 and 5 show compliance with fiscal year 2016 limits for overall CHIMPS and the Crime Victims Fund CHIMP, respectively. This information is used for determining points of order under section 3103 and section 3104, respectively. No full-year bills have been enacted thus far for fiscal year 2016 that include CHIMPS.

In addition to the tables provided by the Senate Budget Committee Republican staff, I am submitting additional

tables from CBO that I will use for enforcement of budget levels agreed to by the Congress.

CBO provided a report for both fiscal year 2015 and fiscal year 2016. This information is used to enforce aggregate spending levels in budget resolutions under section 311 of the CBA. CBO's estimates show that current law levels of spending for fiscal year 2015 exceed the amounts in the deemed budget resolution enacted in the BBA by $8.0 billion in budget authority and $1.0 billion in outlays. Revenues are $79.8 billion below the revenue floor for fiscal year 2015 set by the deemed budget resolution. As well, Social Security outlays are at the levels assumed for fiscal year 2015, while Social Security revenues are $170 million above levels in the deemed budget. This will be CBO's final report to the Senate Budget Committee for fiscal year 2015, as the fiscal year is now closed.

For fiscal year 2016, CBO annualizes the effects of the Continuing Appropriations Act, P.L. 114–53, which provides funding through December 11, 2015. For the enforcement of budgetary aggregates, the Senate Budget Committee excludes this temporary funding. As such, the committee views current law levels as being $885.9 billion and $526.4 billion below budget resolution levels for budget authority and outlays, respectively. Revenues are $144 million above the level assumed in the budget resolution. Finally, Social Security outlays are at the levels assumed in the budget resolution for fiscal year 2016, while Social Security revenues are $18 million above assumed levels for the budget year.

CBO's report also provides information needed to enforce the Senate's pay-as-you-go rule. The Senate's pay-as-you-go scorecard currently shows deficit reduction of $1.4 billion over the fiscal year 2015–2020 period and $6.1 billion over the fiscal year 2015–2025 period. Over the initial 6-year period, Congress has enacted legislation that would increase revenues by $4.1 billion and increase outlays by $2.7 billion. Over the 11-year period, Congress has enacted legislation that would reduce revenues by $1.3 billion and decrease outlays by $7.4 billion. The Senate's pay-as-you-go rule is enforced by section 201 of S. Con. Res. 21, the fiscal year 2008 budget resolution.

All years in the accompanying tables are fiscal years.

I ask unanimous consent that the accompanying tables be printed in the RECORD.

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

TABLE 1.—SENATE AUTHORIZING COMMITTEES—ENACTED DIRECT SPENDING ABOVE (+) OR BELOW (−) BUDGET RESOLUTIONS

(In millions of dollars)

	2015	2016	2016–2020	2016–2025
Agriculture, Nutrition, and Forestry				
Budget Authority	254	0	0	0
Outlays	229	0	0	0
Armed Services				
Budget Authority	−15	0	0	0
Outlays	0	0	0	0
Banking, Housing, and Urban Affairs				
Budget Authority	121	0	0	0
Outlays	121	0	0	0
Commerce, Science, and Transportation				
Budget Authority	0	130	650	1,300
Outlays	0	0	0	0
Energy and Natural Resources				
Budget Authority	0	0	0	0
Outlays	−2	0	0	0
Environment and Public Works				
Budget Authority	0	0	0	−3,160
Outlays	0	0	0	−3,160
Finance				
Budget Authority	7,322	5	13	28
Outlays	7,288	5	13	28
Foreign Relations				
Budget Authority	−20	0	0	0
Outlays	−20	0	0	0
Homeland Security and Governmental Affairs				
Budget Authority	0	0	0	0
Outlays	0	0	0	0
Judiciary				
Budget Authority	0	0	1	2
Outlays	0	0	1	2
Health, Education, Labor, and Pensions				
Budget Authority	3	0	208	278
Outlays	1	0	208	278
Rules and Administration				
Budget Authority	0	0	0	0
Outlays	0	0	0	0
Intelligence				
Budget Authority	0	0	0	0
Outlays	0	0	0	0
Veterans' Affairs				
Budget Authority	0	−2	−1	−1
Outlays	150	388	644	644
Indian Affairs				
Budget Authority	0	0	0	0
Outlays	0	0	0	0
Small Business				
Budget Authority	0	0	0	0
Outlays	0	0	0	0
Total				
Budget Authority	7,665	133	871	−1,553
Outlays	7,767	393	866	−2,208

TABLE 2.—SENATE APPROPRIATIONS COMMITTEE—ENACTED REGULAR DISCRETIONARY APPROPRIATIONS [1]

(Budget authority, in millions of dollars)

	2016	
	Security [2]	Nonsecurity [2]
Statutory Discretionary Limits	523,091	493,491
Amount Provided by Senate Appropriations Subcommittee		
Agriculture, Rural Development, and Related Agencies	0	9
Commerce, Justice, Science, and Related Agencies	0	0
Defense	41	0
Energy and Water Development	0	0
Financial Services and General Government	0	41
Homeland Security	0	9
Interior, Environment, and Related Agencies	0	0
Labor, Health and Human Services, Education and Related Agencies	0	24,678
Legislative Branch	0	0
Military Construction and Veterans Affairs, and Related Agencies	0	56,217
State, Foreign Operations, and Related Programs	0	0
Transportation and Housing and Urban Development, and Related Agencies	0	4,400
Current Level Total	41	85,354
Total Enacted Above (+) or Below (−) Statutory Limits	−523,050	−408,137

[1] This table excludes spending pursuant to adjustments to the discretionary spending limits. These adjustments are allowed for certain purposes in section 251(b)(2) of BBEDCA.

[2] Security spending is defined as spending in the National Defense budget function (050) and nonsecurity spending is defined as all other spending.

TABLE 1.—SENATE AUTHORIZING COMMITTEES—ENACTED DIRECT SPENDING ABOVE (+) OR BELOW (−) BUDGET RESOLUTIONS—Continued

(In millions of dollars)

	2015	2016	2016–2020	2016–2025
Outlays	229	0	0	0
Armed Services				
Budget Authority	−15	0	0	0
Outlays	0	0	0	0
Banking, Housing, and Urban Affairs				
Budget Authority	121	0	0	0
Outlays	121	0	0	0
Commerce, Science, and Transportation				
Budget Authority	0	130	650	1,300
Outlays	0	0	0	0
Energy and Natural Resources				
Budget Authority	0	0	0	0
Outlays	−2	0	0	0
Environment and Public Works				
Budget Authority	0	0	0	−3,160
Outlays	0	0	0	−3,160
Finance				
Budget Authority	7,322	5	13	28
Outlays	7,288	5	13	28
Foreign Relations				
Budget Authority	−20	0	0	0
Outlays	−20	0	0	0
Homeland Security and Governmental Affairs				
Budget Authority	0	0	0	0
Outlays	0	0	0	0
Judiciary				
Budget Authority	0	0	1	2
Outlays	0	0	1	2
Health, Education, Labor, and Pensions				
Budget Authority	3	0	208	278
Outlays	1	0	208	278
Rules and Administration				
Budget Authority	0	0	0	0
Outlays	0	0	0	0
Intelligence				
Budget Authority	0	0	0	0
Outlays	0	0	0	0
Veterans' Affairs				
Budget Authority	0	−2	−1	−1
Outlays	150	388	644	644
Indian Affairs				
Budget Authority	0	0	0	0
Outlays	0	0	0	0
Small Business				
Budget Authority	0	0	0	0
Outlays	0	0	0	0
Total				
Budget Authority	7,665	133	871	−1,553
Outlays	7,767	393	866	−2,208

TABLE 3.—SENATE APPROPRIATIONS COMMITTEE—ENACTED OVERSEAS CONTINGENCY OPERATIONS/GLOBAL WAR ON TERRORISM DISCRETIONARY APPROPRIATIONS

(In millions of dollars)

	2016	
	BA	OT
OCO/GWOT Allocation [1]	96,287	48,798
Amount Provided by Senate Appropriations Subcommittee		
Agriculture, Rural Development, and Related Agencies	0	0
Commerce, Justice, Science, and Related Agencies	0	0
Defense	0	0
Energy and Water Development	0	0
Financial Services and General Government	0	0
Homeland Security	0	0
Interior, Environment, and Related Agencies	0	0
Labor, Health and Human Services, Education and Related Agencies	0	0
Legislative Branch	0	0
Military Construction and Veterans Affairs, and Related Agencies	0	0
State, Foreign Operations, and Related Programs	0	0
Transportation and Housing and Urban Development, and Related Agencies	0	0
Current Level Total	0	0
Total OCO/GWOT Spending vs. Budget Resolution	−96,287	−48,798

BA = Budget Authority; OT = Outlays

[1] This allocation may be adjusted by the Chairman of the Budget Committee to account for new information, pursuant to section 3102 of S. Con. Res. 11, the Concurrent Resolution of the Budget for Fiscal Year 2016.

TABLE 4.—SENATE APPROPRIATIONS COMMITTEE—ENACTED CHANGES IN MANDATORY SPENDING PROGRAMS (CHIMPS)

(Budget authority, millions of dollars)

	2016
CHIMPS Limit for Fiscal Year 2016	19,100
Senate Appropriations Subcommittees	
Agriculture, Rural Development, and Related Agencies	0
Commerce, Justice, Science, and Related Agencies	0
Defense	0
Energy and Water Development	0
Financial Services and General Government	0
Homeland Security	0
Interior, Environment, and Related Agencies	0
Labor, Health and Human Services, Education and Related Agencies	0
Legislative Branch	0
Military Construction and Veterans Affairs, and Related Agencies	0
State, Foreign Operations, and Related Programs	0
Transportation and Housing and Urban Development, and Related Agencies	0
Current Level Total	0
Total CHIMPS Above (+) or Below (−) Budget Resolution	−19,100

TABLE 5.—SENATE APPROPRIATIONS COMMITTEE—ENACTED CHANGES IN MANDATORY SPENDING PROGRAM (CHIMP) TO THE CRIME VICTIMS FUND

(Budget authority, millions of dollars)

	2016
Crime Victims Fund (CVF) CHIMP Limit for Fiscal Year 2016	10,800
Senate Appropriations Subcommittees	
Agriculture, Rural Development, and Related Agencies	0
Commerce, Justice, Science, and Related Agencies	0
Defense	0
Energy and Water Development	0
Financial Services and General Government	0
Homeland Security	0
Interior, Environment, and Related Agencies	0
Labor, Health and Human Services, Education and Related Agencies	0
Legislative Branch	0
Military Construction and Veterans Affairs, and Related Agencies	0
State Foreign Operations, and Related Programs	0
Transportation and Housing and Urban Development, and Related Agencies	0
Current Level Total	0
Total CVF CHIMP Above (+) or Below (−) Budget Resolution	−10,800

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, October 27, 2015.

Hon. MIKE ENZI,
Chairman, Committee on the Budget,
U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The enclosed report shows the effects of Congressional action on the fiscal year 2015 budget and is current through September 30, 2015. This report is submitted under section 308(b) and in aid of section 311 of the Congressional Budget Act, as amended.

The estimates of budget authority, outlays, and revenues are consistent with the allocations, aggregates, and other budgetary levels printed in the Congressional Record on May 5, 2014, pursuant to section 116 of the Bipartisan Budget Act (Public Law 113–67).

Since our last letter dated September 10, 2015, there has been no Congressional action affecting budget authority, outlays, or revenues for fiscal year 2015.

Sincerely,

KEITH HALL, *Director*.

Enclosure.

TABLE 1.—SENATE CURRENT LEVEL REPORT FOR SPENDING AND REVENUES FOR FISCAL YEAR 2015, AS OF SEPTEMBER 30, 2015

[In billions of dollars]

	Budget Resolution	Current Level [a]	Current Level Over/Under (−) Resolution
On-Budget			
Budget Authority	3,026.4	3,034.4	8.0
Outlays	3,039.6	3,040.7	1.0
Revenues	2,533.4	2,453.6	−79.8
Off-Budget			
Social Security Outlays [b]	736.6	736.6	0.0
Social Security Revenues	771.7	771.9	0.2

Source: Congressional Budget Office.

[a] Excludes amounts designated as emergency requirements.

[b] Excludes administrative expenses paid from the Federal Old-Age and Survivors Insurance Trust Fund and the Federal Disability Insurance Trust Fund of the Social Security Administration, which are off-budget, but are appropriated annually.

TABLE 2.—SUPPORTING DETAIL FOR THE SENATE CURRENT LEVEL REPORT FOR ON-BUDGET SPENDING AND REVENUES FOR FISCAL YEAR 2015, AS OF SEPTEMBER 30, 2015

[In millions of dollars]

	Budget Authority	Outlays	Revenues
Previously Enacted [a]			
Revenues	n.a.	n.a.	2,533,388
Permanents and other spending legislation	1,877,558	1,802,360	n.a.
Appropriation legislation	0	508,261	n.a.
Offsetting receipts	−735,195	−734,481	n.a.
Total, Previously Enacted	1,142,363	1,576,140	2,533,388
Enacted Legislation: [b]			
Lake Hill Administrative Site Affordable Housing Act (P.L. 113–141)	0	−2	0
Emergency Supplemental Appropriations Resolution, 2014 (P.L. 113–145)	0	75	0
Highway and Transportation Funding Act of 2014 (P.L. 113–159)	0	−15	2,590
Emergency Afghan Allies Extension Act of 2014 (P.L. 113–160)	5	5	6
Continuing Appropriations Resolution, 2015 (P.L. 113–164) [c]	−4,705	−180	0
Preventing Sex Trafficking and Strengthening Families Act (P.L. 113–183)	0	10	0
IMPACT Act of 2014 (P.L. 113–185)	22	22	0
Consolidated and Further Continuing Appropriations Act, 2015 (P.L. 113–235)	1,884,271	1,426,085	−178
An act to amend certain provisions of the FAA Modernization and Reform Act of 2012 (P.L. 113–243)	0	0	−28
Naval Vessel Transfer Act of 2013 (P.L. 113–276)	−20	−20	0
Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015 (P.L. 113–291)	−15	0	0
An act to amend the Internal Revenue Code of 1986 to extend certain expiring provisions and make technical corrections, to amend the Internal Revenue Code of 1986 to provide for the treatment of ABLE accounts established under State programs for the care of family members with disabilities, and for other purposes (P.L. 113–295)	160	160	−81,177
Terrorism Risk Insurance Program Reauthorization Act of 2015 (P.L. 114–1)	121	121	1
Department of Homeland Security Appropriations Act, 2015 (P.L. 114–4)	47,763	27,534	0
Medicare Access and CHIP Reauthorization Act of 2015 (P.L. 114–10)	7,354	7,329	0
Construction Authorization and Choice Improvement Act (P.L. 114–19)	0	20	0
An act to extend the authorization to carry out the replacement of the existing medical center of the Department of Veterans Affairs in Denver, Colorado, to authorize transfers of amounts to carry out the replacement of such medical center, and for other purposes (P.L. 114–25)	0	130	0
Trade Preferences Extension Act of 2015 (P.L. 114–27)	38	7	−1,051
Surface Transportation and Veterans Health Care Choice Improvement Act of 2015 (P.L. 114–41) [b]	0	0	19
Total, Enacted Legislation	1,934,994	1,461,281	−79,818
Entitlements and Mandatories:			
Budget resolution estimates of appropriated entitlements and other mandatory programs	−42,921	3,239	0
Total Current Level [d]	3,034,436	3,040,660	2,453,570
Total Senate Resolution [e]	3,026,439	3,039,624	2,533,388
Current Level Over Senate Resolution	7,997	1,036	n.a.
Current Level Under Senate Resolution	n.a.	n.a.	79,818

Source: Congressional Budget Office.

Notes: n.a. = not applicable; P.L. = Public Law.

[a] Includes the following acts that affect budget authority, outlays, or revenues, and were cleared by the Congress during the 2nd session of the 113th Congress but before publication in the Congressional Record of the statement of the allocations and aggregates pursuant to section 116 of the Bipartisan Budget Act of 2013 (P.L. 113–67): the Agricultural Act of 2014 (P.L. 113–79), the Homeowner Flood Insurance Affordability Act of 2014 (P.L. 113–89), the Gabriella Miller Kids First Research Act (P.L. 113–94), and the Cooperative and Small Employer Charity Pension Flexibility Act (P.L. 113–97).

[b] Pursuant to section 403(b) of S. Con. Res. 13, the Concurrent Resolution on the Budget for Fiscal Year 2010, amounts designated as an emergency requirement pursuant to section 403 of S. Con. Res. 13, shall not count for certain budgetary enforcement purposes. The amounts so designated for 2015, which are not included in the current level totals, are as follows:

	Budget Authority	Outlays	Revenues
Veterans' Access to Care through Choice, Accountability, and Transparency Act of 2014 (P.L. 113–146)	−1,331	6,619	−42
Surface Transportation and Veterans Health Care Choice Improvement Act of 2015 (P.L. 114–41) –	0	1,147	0
Total, amounts designated pursuant to Sec. 403 of S. Con. Res. 13	−1,331	7,766	−42

[c] Sections 136 and 137 of the Continuing Appropriations Resolution, 2015 (P.L. 113–164) provide $88 million to respond to the Ebola virus, which is available until September 30, 2015. Section 139 rescinds funds from the Children's Health Insurance Program. Section 147 extended the authorization for the Export-Import Bank of the United States through June 30, 2015.

[d] For purposes of enforcing section 311 of the Congressional Budget Act in the Senate, the budget resolution does not include budget authority, outlays, or revenues for off-budget amounts. As a result, current level does not include these items.

[e] Periodically, the Senate Committee on the Budget revises the budgetary levels printed in the Congressional Record on May 5, 2014, pursuant to section 116 of the Bipartisan Budget Act of 2013 (Public Law 113–67):

	Budget Authority	Outlays	Revenues
Original Senate Resolution:	2,939,993	3,004,163	2,533,388
Revisions:			
Adjustment for Disaster Designated Spending	100	43	0
Adjustment for Overseas Contingency Operations and Disaster Designated Spending	74,995	31,360	0
Adjustment for Emergency Designated Spending	0	75	0
Adjustment for the Consolidated and Further Continuing Appropriations Act, 2015	11,351	3,983	0
Revised Senate Resolution	3,026,439	3,039,624	2,533,388

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, October 27, 2015.

Hon. MIKE ENZI,
Chairman, Committee on the Budget,
U.S. Senate Washington, DC.

DEAR MR. CHAIRMAN: The enclosed report shows the effects of Congressional action on the fiscal year 2016 budget and is current through October 26, 2015. This report is submitted under section 308(b) and in aid of section 311 of the Congressional Budget Act, as amended.

The estimates of budget authority, outlays, and revenues are consistent with the technical and economic assumptions of S. Con. Res. 11, the Concurrent Resolution on the Budget for Fiscal Year 2016.

Since our last letter dated September 10, 2015, the Congress has cleared and the President has signed the following acts that affect budget authority, outlays, or revenues for fiscal year 2016: Continuing Appropriations Act, 2016 (Public Law 114–53); Airport and Airway Extension Act of 2015 (Public Law 114–55); Department of Veterans Affairs Expiring Authorities Act of 2015 (Public Law 114–58); and Protecting Affordable Coverage for Employees Act (Public Law 114–60).

Sincerely,

KEITH HALL, *Director*.

Enclosure.

TABLE 1.—SENATE CURRENT LEVEL REPORT FOR SPENDING AND REVENUES FOR FISCAL YEAR 2016, AS OF OCTOBER 26, 2015

[In billions of dollars]

	Budget Resolution [a]	Current Level [b]	Current Level Over/Under (−) Resolution
ON-BUDGET			
Budget Authority	3,033.5	3,155.6	122.1
Outlays	3,092.0	3,167.9	76.0
Revenues	2,676.0	2,676.1	0.1
OFF-BUDGET			
Social Security Outlays [c]	777.1	777.1	0.0
Social Security Revenues	794.0	794.0	0.0

Source: Congressional Budget Office.

[a] Excludes $6,872 million in budget authority and $344 million in outlays assumed in S. Con. Res. 11 for disaster-related spending that is not yet allocated to theSenate Committee on Appropriations.

[b] Excludes amounts designated as emergency requirements.

[c] Excludes administrative expenses paid from the Federal Old-Age and Survivors Insurance Trust Fund and the Federal Disability Insurance Trust Fund of the Social Security Administration, which are off-budget, but are appropriated annually.

TABLE 2.—SUPPORTING DETAIL FOR THE SENATE CURRENT LEVEL REPORT FOR ON-BUDGET SPENDING AND REVENUES FOR FISCAL YEAR 2016, AS OF OCTOBER 26, 2015

[In millions of dollars]

	Budget Authority	Outlays	Revenues
Previously Enacted [a]			
Revenues	n.a.	n.a.	2,676,733
Permanents and other spending legislation	1,968,496	1,902,345	n.a.
Appropriation legislation	0	500,825	n.a.
Offsetting receipts	−784,820	−784,879	n.a.
Total, Previously Enacted	1,183,676	1,618,291	2,676,733
Enacted Legislation:			
An act to extend the authorization to carry out the replacement of the existing medical center of the Department of Veterans Affairs in Denver, Colorado, to authorize transfers of amounts to carry out the replacement of such medical center, and for other purposes (P.L. 114–25)	0	20	0
Defending Public Safety Employees' Retirement Act & Bipartisan Congressional Trade Priorities and Accountability Act of 2015 (P.L. 114–26)	0	0	5
Trade Preferences Extension Act of 2015 (P.L. 114–27)	445	175	−766
Steve Gleason Act of 2015 (P.L. 114–40)	5	5	0
Surface Transportation and Veterans Health Care Choice Improvement Act of 2015 (P.L. 114–41) [b]	0	0	99
Continuing Appropriations Act, 2016 (P.L. 114–53)	700	775	0
Airport and Airway Extension Act of 2015 (P.L. 114–55)	130	0	0
Department of Veterans Affairs Expiring Authorities Act of 2015 (P.L. 114–58)	−2	368	0
Protecting Affordable Coverage for Employees Act (P.L. 114–60)	0	0	40
Total, Enacted Legislation	1,278	1,343	−622
Continuing Resolution:			
Continuing Appropriations Act, 2016 (P.L. 114–53)	1,008,053–	602,405 –	0
Entitlements and Mandatories:			
Budget resolution estimates of appropriated entitlements and other mandatory programs	962,619	945,910	0
Total Current Level [c]	3,155,626	3,167,949	2,676,111
Total Senate Resolution [d]	3,033,488	3,091,973	2,675,967
Current Level Over Senate Resolution	122,138	75,976	144
Current Level Under Senate Resolution	n.a.	n.a.	n.a.
Memorandum: Revenues, 2016–2025:			
Senate Current Level	n.a.	n.a.	32,237,119
Senate Resolution	n.a.	n.a.	32,233,099
Current Level Over Senate Resolution	n.a.	n.a.	4,020
Current Level Under Senate Resolution	n.a.	n.a.	n.a.

Source: Congressional Budget Office.

Notes: n.a. = not applicable; P.L. = Public Law.

[a] Includes the following acts that affect budget authority, outlays, or revenues, and were cleared by the Congress during this session, but before the adoption of S. Con. Res. II, the Concurrent Resolution on the Budget for Fiscal Year 2016: the Terrorism Risk Insurance Program Reauthorization Act of 2014 (P.L. 114–41); the Department of Homeland Security Appropriations Act, 2015 (P.L. 114–4), and the Medicare Access and CHIP Reauthorization Act of 2015 (P.L. 114–10).

[b] Pursuant to section 403(b) of S. Con. Res. 13, the Concurrent Resolution on the Budget for Fiscal Year 2010, amounts designated as an emergency requirement pursuant to section 403 of S. Con. Res. 13, shall not count for certain budgetary enforcement purposes. The amounts so designated for 2016, which are not included in the current level totals, are as follows:

	Budget Authority	Outlays	Revenues
Surface Transportation and Veterans Health Care Choice Improvement Act of 2015 (P.L. 114–41)	0	917	0

[c] For purposes of enforcing section 311 of the Congressional Budget Act in the Senate, the resolution, as approved by the Senate, does not include budget authority, outlays, or revenues for off-budget amounts. As a result, current level does not include these items.

[d] Periodically, the Senate Committee on the Budget revises the budgetary levels in S. Con Res. 11 , pursuant to various provisions of the resolution. The Senate Resolution total below excludes $6,872 million in budget authority and $344 million in outlays assumed in S. Con Res. 11 for disaster-related spending that is not yet allocated to the Senate Committee on Appropriations:

	Budget Authority	Outlays	Revenues
Senate Resolution:	3,032,343	3,091,098	2,676,733
Revisions:			
Pursuant to section 4311 of S. Con. Res. 11	445	175	−766
Pursuant to section 311 of S. Con. Res. 11	700	700	0
Revised Senate Resolution	3,033,488	3,091,973	2,675,967

TABLE 3.—SUMMARY OF THE SENATE PAY-AS-YOU-GO SCORECARD FOR THE 114TH CONGRESS—1ST SESSION, AS OF OCTOBER 26, 2015

(In millions of dollars)

	2015–2020	2015–2025
Beginning Balance [a]	0	0
Enacted Legislation: [b c d]		
Iran Nuclear Agreement Review Act of 2015 (P.L. 114–17) [e]	n.e.	n.e.
Construction Authorization and Choice Improvement Act (P.L. 114–19)	20	20
Justice for Victims of Trafficking Act of 2015 (P.L. 114–22)	1	2
Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (P.L. 114–23)	*	*
An act to extend the authorization to carry out the replacement of the existing medical center of the Department of Veterans Affairs in Denver, Colorado (P.L. 114–25)	150	150
Defending Public Safety Employees' Retirement Act & Bipartisan Congressional Trade Priorities and Accountability Act of 2015 (P.L. 114–26)	−1	5
Trade Preferences Extension Act of 2015 (P.L. 114–27)	−640	−52
Boys Town Centennial Commemorative Coin Act(P.L. 114–30) [f]	0	0
Steve Gleason Act of 2015 (P.L. 114–40)	13	28
Surface Transportation and Veterans Health Care Choice Improvement Act of 2015 (P.L. 114–41)	−1,552	−6,924
Agriculture Reauthorizations Act of 2015 (P.L. 114–54)	*	*
Department of Veterans Affairs Expiring Authorities Act of 2015 (P.L. 114–58)	624	624
Protecting Affordable Coverage for Employees Act (P.L. 114–60)	−32	−2
Gold Star Fathers Act of 2015 (P.L. 114–62)	*	*
Ensuring Access to Clinical Trials Act of 2015 (P.L. 114–63)	*	*
Adoptive Family Relief Act (P.L. 114–70)	*	*
Illegal, Unreported, and Unregulated Fishing Enforcement Act of 2015 (H.R. 774)	*	*
A bill to amend title XI of the Social Security Act to clarify waiver authority regarding programs of all-inclusive care for the elderly (PACE programs) (S. 1362)	*	*
Current Balance	−1,417	−6,149
Memorandum:		
	2015–2020	2015–2025
Changes to Revenues	4,140	−1,284
Changes to Outlays	2,723	−7,433

Source: Congressional Budget Office.

Notes: n.e. = not able to estimate; P.L. = Public Law. * = between −$500,000 and $500,000.

[a] Pursuant to S. Con. Res. 11, the Senate Pay-As-You-Go Scorecard was reset to zero.

[b] The amounts shown represent the estimated impact of the public laws on the deficit. Negative numbers indicate an increase in the deficit; positive numbers indicate a decrease in the deficit.

[c] Excludes off-budget amounts.

[d] Excludes amounts designated as emergency requirements.

[e] P.L. 114–17 could affect direct spending and revenues, but such impacts would depend on future actions of the President that CBO cannot predict. (http://www.cbo.gov/sites/det1mltlfiles/cbofiles/attachments/s615.pdf)

[f] P.L. 114–30 will cause a decrease in spending of $5 million in 2017 and an increase in spending of $5 million in 2019 for a net impact of zero over the six-year and eleven-year periods.

EPA GOLD KING MINE SPILL

Mr. MCCAIN. Mr. President, last month the Senate Indian Affairs Committee held an oversight hearing on the Environmental Protection Agency's Gold King Mine disaster. I am very grateful that Chairman JOHN BARRASSO and Vice Chairman JON TESTER quickly made this matter a priority for their committee following the August break. The hearing focused on the harmful impacts that spill is having on Indian Country, namely the Navajo Nation, the Southern Ute Tribe, and the Ute Mountain Ute Tribe.

On the Navajo Nation, an estimated 1,500 farms have been damaged by the EPA and its contractors when they released a deluge of tailings-pond wastewater from the abandoned Gold King Mine. On August 5, 2015, an acidic plume of mercury, arsenic, and other metals worked its way down the Animas River in Colorado and into the San Juan River near Farmington, NM. Nobody yet knows for certain the total damage to crops, soil, livestock, wildlife, and water supplies that are critical sources of food for the Navajo people and also serve as economic and cultural centers. Those farmers who were able to shut down their irrigation systems watched in horror as their crops wilted.

The EPA now says water quality in the San Juan River has returned to ''pre-event levels,'' but the Gold King Mine is still releasing water roughly at 600 gallons per minute. The concentrations of toxic metals may not as be as high today as it was during the initial 3 million gallon flush, but the Navajo are still waiting for EPA to demonstrate it can prevent another large release. The nation is rightfully demanding assurances that heavy rainfall won't disturb toxic substances that may have settled in the sediment of the Animas River, the San Juan River, or even Lake Powell.

In August, I—along with Arizona Governor Doug Ducey—met with Navajo Nation president Russell Begaye and Navajo council speaker Lorenzo Bates in Window Rock, AZ, to discuss this matter. I can assure my colleagues that the Navajo are suffering deeply and dearly because of this spill. I have also received calls and letters from a number of concerned constituents, mayors, county supervisors, and businesses in northern Arizona who also have a stake in the health and safety of Lake Powell. They are just as alarmed as the Navajo people that the plume could endanger their livelihoods and their enjoyment of natural resources in their communities. The Arizona Department of Environmental Quality and the Arizona Geological Survey have been expending scarce resources to conduct water samples independent of EPA. And that has been helpful. But the Federal Government has to step up and take action that would allow all affected stakeholders, but especially tribal communities, find confidence in what the Federal Government is doing to fix the mess that it created.

At last month's hearing, we received testimony from EPA Administrator Gina McCarthy and others dealing with the spill, including the Navajo Nation president, Russell Begaye. We also received testimony from Doug Holtz-Eakin, a noted economist and former Director of the Congressional Budget Office. Mr. Holtz-Eakin estimated that the spill will cost the Navajo's agriculture sector roughly $41,000 a day in lost economic activity.

While I am grateful that Administrator McCarthy agreed to appear before the committee, I am concerned that, under her watch, not a single Agency employee or contractor had been fired for the disaster. In her testimony, Administrator McCarthy portrayed the EPA's response to the tribes as timely, but her portrayal was directly contradicted by the testimony of the Navajo president, who noted that it took EPA 2 days to notify the tribe about the plume's threat to the tribe. It was also revealed that Administrator McCarthy did not directly contact President Begaye for about 5 days after the spill. The committee also received testimony that EPA had not quickly and routinely shared water monitory data with the tribes. All of this shatters any notion that EPA has honored its government-to-government responsibility to the nation.

The Gold King Mine spill was a series of failures by EPA that compounded, and the Navajo are paying the price. I will continue to push for increased congressional oversight into this matter.

HEAD START AWARENESS MONTH

Mr. CARPER. Mr. President, it is with great pleasure that I speak on behalf of the Delaware delegation to honor Head Start's 50 years of service to our Nation's most vulnerable children and families in Delaware and nationwide. On May 18, 1965, President Lyndon B. Johnson launched Project Head Start as an 8-week summer demonstration project to teach low-income students needed skills before they started kindergarten. Over the past 50 years, Head Start has served 32 million children and families across the country with comprehensive services.

The Head Start Program has given children and families the tools to succeed by ensuring a high quality education and access to health care and social services. The Head Start Program represents a critical investment in the education of our nation's youngest children. In the State of Delaware, 2,714 children and pregnant women benefitted from Head Start, Early Head Start, and the Early Childhood Assistance Program in 2014. Head Start is instrumental in uplifting families in Delaware by providing resources to families who, like many of us, want to see their children reach their full potential.

The teachers, home visitors, and family service workers that make up the Head Start Program are the backbone of this mission. Without them on the front lines each and every day, these early education goals would not be met. I commend the teachers and staff who are deeply committed to seeing all children succeed. On behalf of Senator CHRIS COONS and Congressman JOHN CARNEY, I recognize Head Start Awareness Month and the 50th Anniversary of Head Start. It is our sincere hope that future generations of children and families can continue to greatly benefit from Head Start's programs and we can put children on the right path from the very beginning.

OBSERVING INTERNATIONAL DAY OF THE GIRL

Mr. KIRK. Mr. President, October 11 marked the second annual International Day of the Girl. This day

brings together people and advocacy groups to raise awareness about the challenges facing girls around the world. Tragically, today's regional crises are having a disproportionately destructive impact on girls. 2015 marks the year with the highest number of displaced persons since World War II. According to the United Nations High Commissioner for Refugees, women and girls comprise half of any refugee or internally displaced population. Crises such as the ongoing conflict in Syria, over 1.5 million displaced in South Sudan, and the expanding migrant crisis in Europe, among others, risk leaving an entire generation of girls shaped by a lack of opportunity, gender-based violence, forced marriage, and disrupted education.

Access to education is often a top priority for refugee families upon resettling in a foreign country. We know that, if empowered with the appropriate tools, girls can be facilitators of change who can transform their own lives, as well as the lives of their families, communities, and societies and serve as a bulwark against the conditions that contribute to extremism that so many terrorist groups have exploited, often at the expense of women and girls. The lack of access to education for refugee girls stifles empowerment and stands in the way of achieving a durable solution to conflict.

As the United States and the international community work to cope with the current refugee crisis, it is critical that we focus not only on security but on the basic needs of refugees, such as access to education and increasing the role of women and girls in humanitarian response and civil society programs.

TRIBUTE TO THOMAS ROCKROADS, JR.

Mr. TESTER. Mr. President, I wish to honor Thomas Rockroads, Jr., a veteran of the Vietnam war. On behalf of all Montanans and all Americans, I would like to thank Mr. Rockroads for his service to our State and to our Nation. It is my privilege to share Thomas's story for the official Senate Record.

Thomas Rockroads, Jr., was born on December 21, 1948, in Crow Agency, MT. His father worked in sawmills in both Kirby and Lame Deer and was a ranch hand and coal miner in Lame Deer. His mother worked for many years at the Northern Hotel before coming home to the Northern Cheyenne Reservation. He spent his childhood in Busby and attended Busby High School until joining the Army his junior year.

In September of 1968, he volunteered for the Army Airborne Infantry, and by September of 1969, he found himself jumping out of helicopters and into the highlands of Vietnam. Thomas was a member of the 173rd Airborne Brigade, which was stationed in the hot, humid Tiger Mountains of Vietnam's Central Highlands. Their responsibilities included rescuing and evacuating ground forces, as well as setting up perimeters for operations. They were right in the thick of things, and, as Thomas once put it, ''If there was a hot spot where reinforcements were needed . . . we were there.'' On more than one occasion, this proved to be an important but harrowing position to be in. One night, when the brigade was charged with setting up a perimeter on a hillside, Thomas and his comrades felt particularly concerned. They knew the area was likely heavily booby-trapped, so they proceeded with extra caution. Their mission was to intercept the North Vietnamese forces headed in their direction, and after establishing a perimeter, they were allowed a few hours of rest before being put on high alert. A few hours later, while he was trying to get some sleep, Thomas suddenly heard a blast, and he was thrown nearly a dozen feet from his makeshift tent. Thomas quickly realized that someone had set off a booby trap, but before he could process much else, a medic began calling his name and he rushed over to help. Thomas worked with the medic to care for his fellow soldier, but shortly thereafter the man died in Thomas's arms.

A few days later, Thomas and his brigade found themselves under siege again—this time, without cover, they came face to face with enemy soldiers. The North Vietnamese troops, equipped with an anti-aircraft gun and hiding inside an irrigation trench, began rapid firing on Thomas and his platoon. Knowing they needed air support, Thomas headed right toward the anti-aircraft gun—as long as it was operable, American helicopters couldn't access the area. However, his M16 was jammed, so under heavy fire, he had to dislodge the trapped bullets and replace them with a new magazine. He and a fellow solider finally located the enemy's weapon at the far end of a hedgerow and headed back into the firestorm with one aim—to disarm it. Before they could reach their target, an enemy solider intercepted them, lobbing a grenade directly at Thomas and his comrade. They both ran for cover, and thankfully the grenade failed to detonate, but mere seconds after that, another soldier charged them, firing wildly at Thomas and his platoon. The soldier was not more than 10 feet away from Thomas when he finally went down.

Thomas returned to Busby, MT, a full 365 days after his deployment. He remarkably didn't sustain a single scratch. But like many of his fellow veterans, despite his lack of visible wounds, Thomas has struggled with the unseen wounds of war. Thirty-five years after coming back from Vietnam, he was formally diagnosed with post-traumatic stress disorder.

Despite this often debilitating struggle, Thomas has spent the last 30 years working for Western Energy's Rosebud Mine at Colstrip and raising two daughters and a son with his wife, Charlotte, of 38 years. He also has grandchildren. He credits his family with helping him heal. ''It's all the support of my family that's got me where I'm at today,'' Thomas said. ''My wife is always supporting me. My daughters, my son and my grandchildren—I'm very, very fortunate.''

However, Thomas is still haunted by his memories daily, and he doesn't want other soldiers to have to suffer the way he has had to. He believes, like I do, that our commitment to our veterans is a cost of war, and we must make it a priority to help, protect, and serve those who served. Too many of our Vietnam veterans never got the homecoming or the recognition they deserved. So today I am honored to have the opportunity to thank Thomas for his bravery both in battle and beyond. He is a Montanan born and bred, and his life has been a testament to the kind of commitment, courage, and compassion that our State can be proud of.

It was my honor to recognize Thomas Rockroads, Jr. by presenting him with the Bronze Star Medal, National Defense Service Medal, Vietnam Service Medal, Combat Infantryman Badge 1st Award, Republic of Vietnam Campaign Ribbon with 1960 Device, Sharpshooter Badge with auto rifle bar with rifle bar, Marksman Badge with machine gun bar, and the Parachutist Badge Basic.

Our State and our Nation thank you, Thomas, for your service and for a soldier's sacrifice.

RECOGNIZING MENTOR: THE NATIONAL MENTORING PARTNERSHIP

Mr. BOOKER. Mr. President, today I would like to recognize MENTOR: The National Mentoring Partnership, the leadership of its founders, Geoffrey T. Boisi and Raymond G. Chambers, and the expansion of the mentoring field in the past quarter century.

This year, MENTOR celebrates its 25th anniversary. Its founders, Geoffrey T. Boisi and Raymond G. Chambers, were leading businessmen and philanthropists who understood the value of mentoring in their own lives. They believed passionately that the intervention of a caring adult is a critical element in the life of a young person, and they believed that every young person needs and deserves a powerful relationship that supports their growth and gives them the opportunity for success.

In 1990, Boisi and Chambers recognized the powerful impact that mentoring could have on our Nation's at-risk youth, and they started a movement to increase opportunity for all young people by establishing MENTOR. The success of Boisi's and Chambers' efforts has been remarkable. That first year, approximately 300,000 youth at risk of falling off track were paired with a caring adult through a structured mentoring program. Today, 4.5 million at-risk young people will find

the support that they need in a mentoring relationship while growing up.

We know that research has found that young people with a mentor are 55 percent more likely to attend college and more than twice as likely to say that they held a leadership position in a club or sports team than young people without mentors. We also know that people who are mentored in their youth are 78 percent more likely to volunteer in their communities than those who are not mentored.

Unfortunately, despite the tremendous growth of the mentoring movement in America over the past 25 years, 1 in 3 young people, including 9 million at-risk youth, will still reach adulthood without having a mentor of any kind. This mentoring gap isolates these young people from the meaningful connections to adults that would help them to grow and succeed. Furthermore, young people are not the only ones who gain from a mentoring relationship. While mentoring empowers our children and sets them on the path to success, it also deeply enriches the lives of the adults who are partnered with them. As a mentor myself, I can attest to this profound benefit.

MENTOR has been a leader in the development of best practices to assist mentoring organizations across the country in improving their program quality. MENTOR and its network of affiliate Mentoring Partnerships has set the bar for quality in practice and has strengthened the mentoring field's capacity to deliver on the promise of mentoring.

It is clear that, in the last quarter century, MENTOR, under the leadership of its volunteer board and founders, has done tremendous work championing the advancement of mentoring practice and fostering the growth of the mentoring movement. Therefore, I ask that my colleagues join me in recognizing the accomplishments of this remarkable organization in expanding the quality and availability of mentoring for all young people in the United States, in honoring the service and leadership of MENTOR cofounders Geoffrey T. Boisi and Raymond G. Chambers and their dedication to America's youth, and in encouraging Americans to discover just how rewarding mentoring can be through volunteering with their local mentoring organization.

ADDITIONAL STATEMENTS

TRIBUTE TO REVEREND DOCTOR M. WILLIAM HOWARD, JR.

● Mr. BOOKER. Mr. President, today I would like to recognize Rev. Dr. M. William Howard, Jr., pastor of Newark's Bethany Baptist Church. Dr. Howard has spent many decades leading the charge for change, fueled by his personal mission to utilize his faith to transform the human condition.

From his Georgia roots to his work at Bethany Baptist, Dr. Howard has shown an extraordinary commitment to serving others. His work outside of the church has spanned the realms of human rights, international affairs, domestic policy, and education. In his role over the last 15 years as pastor of Bethany Baptist Church, he has worked tirelessly to expand outreach to the community as a whole.

Since his first position as a youth leader conducting some of the earliest voter outreach efforts in southwest Georgia, Dr. Howard has been a beacon of light across the globe, bridging the worlds of faith and political activism. He has consistently taken on leadership roles, serving as moderator of the Programme to Combat Racism of the World Council of Churches, president of the National Council of Churches, and president of the American Committee on Africa. Through these posts, Dr. Howard has provided a powerful example of our Nation's commitment to human rights and equality. In ministering to U.S. personnel held hostage in Iran in 1979 and working for the release of U.S. Navy pilot Robert O. Goodman, Dr. Howard was a quiet but powerful force for faith and peace.

Dr. Howard's record of service and leadership domestically is equally impressive. Serving as president of New York Theological Seminary, he demonstrated the importance of interdisciplinary approaches to community development by implementing joint programs in social work and urban education. He has been a board member for such organizations as the National Urban League, the Children's Defense Fund, and the Rutgers University Board of Governors. Under his leadership, the New Jersey Death Penalty Study Commission was instrumental in New Jersey becoming the first State to abolish the death penalty since 1976.

Finally, Dr. Howard's impact on the city of Newark has been remarkable. As pastor of Bethany, Dr. Howard quickly established Bethany Cares, Inc., and through this outreach corporation, the church has actively transcended its congregation walls to serve the community at large. Such transformative work has played an integral part in strengthening the development of New Jersey's largest city.

After 15 years of devoted service as pastor of Bethany Baptist Church, Dr. Howard will be retiring. It is an honor to formally recognize Dr. Howard for his unwavering commitment to creating a better world.●

RECOGNIZING VFW POST 1674 ON ITS 75TH ANNIVERSARY

● Mr. BOOZMAN. Mr. President, I wish to honor Veterans of Foreign Wars Post 1674 in Siloam Springs, AR, on its 75th anniversary.

Chartered November 10, 1940, the post was named in honor of Levi Douthit, a WWI veteran.

As a member of the Committee on Veterans' Affairs, I understand the importance of acknowledging the bravery and valor of the men and women who fought in defense of our country, as well as those who continue to serve. Men like Levi Douthit and members of VFW Post 1674 set their personal lives aside to fight for our country. This post recognizes the service, sacrifice, and courage of fellow veterans and continues to offer aid and assistance to those who served our Nation in uniform.

As participants in the Buddy Poppy Program, members support the veterans relief fund. They serve veterans in and around Siloam Springs who need help with daily basic needs and transportation to VA health centers for medical treatments.

Members continue their dedication to the community, offering scholarships to students, teaching flag etiquette, and, as partners with Kind at Heart Ministries of Siloam Springs, helping build wheelchair ramps for veterans.

The importance of Post 1674 to the community was apparent when more than a decade ago a lack of membership and financial troubles nearly forced its closure. Businessmen helped raise support in the community and kept its doors open.

I congratulate VFW Post 1674 on its 75th anniversary. I wish Commander Frank Lee and the 163 members who served in U.S. engagements since WWII the best of luck and many more years of camaraderie, service, and investment in the community.●

50-YEAR CLASS REUNION OF THE 1965 CLASS OF WESTERN HIGH SCHOOL

● Mr. CARDIN. Mr. President, this week in my hometown of Baltimore, MD, the Western High School class of 1965 will gather to celebrate their 50th class reunion. In honor of this special occasion, I wish to take a moment to pay tribute to the experiences of the WHS class of 1965 and commemorate the lasting legacy of Western High School, which continues to produce leaders for the Baltimore community.

To this day, Western High School remains a source of pride for the city of Baltimore. Founded as Western Female High School in 1844, it remains the oldest operating public all-girls high school in the Nation nearly 171 years after its doors opened on North Paca Street. Prior to the opening of Western Female High School and its now defunct companion Eastern Female High School, Baltimore City females were without an opportunity to advance their education beyond the basic grammar school level. Female students from across the city were drawn to the academic rigor of Western High School, creating a true magnet school, as we know today. As the city of Baltimore grew, so did Western High School. In 1896, Western High School moved to a larger location on Lafayette and McCulloh Streets, which allowed for

the expansion of courses to include clerical courses. Today Western High School resides on a joint campus opened in 1967 with the all-male Baltimore Polytechnic Institute on Falls Road.

The WHS class of 1965 graduated from Western in a transitionary period for Western. Two years away from the opening of the current campus, Western High School students attended classes in the heart of downtown Baltimore. With an overpopulated school building that forced administrators to move to a split shift schedule to accommodate all of Western's students, alumnae often participated in work or volunteer opportunities located within walking distance of the school. This proximity to downtown also allowed Western students to participate in the burgeoning civil rights movement in Baltimore City, including the picketing of businesses which refused to serve African Americans. While Western High School students can fondly remember their efforts to fight for social justice in the civil rights movement, the class of 1965 was also struck by the tragic news of President John F. Kennedy's assassination. Even as WHS mourned this news, former Western High School alumna Sarah T. Hughes, then judge of the U.S. District Court for the Northern District of Texas and just the third woman to ever serve as a Federal jurist, administered the oath of office to then-Vice President Lyndon B. Johnson aboard Air Force One.

The storied history of Western High School and school motto, ''Lucem accepimus, lucem demus''—''We have received light, let us give light''—has continued to inspire generations of students and countless alumnae of WHS. Among its alumnae include Henrietta Szold, the founder of Hadassah; Trazana Beverley, a 1977 Tony Award Winner; former Maryland State superintendent of schools Dr. Nancy S. Grasmick; current Baltimore City mayor Stephanie Rawlings-Blake; and current Western High School principal Michelle White. As the WHS class of 1965 comes together this week to celebrate their class reunion and years of friendship, I encourage each alumnae to remember the words they were taught at Western High School many years ago and continue to strengthen their own communities.●

TRIBUTE TO JAMIE TURNER

● Mr. CARPER. Mr. President, it is with great pleasure that, on behalf of the Delaware congressional delegation, I wish to honor the exemplary service of Jamie Turner, director of the Delaware Emergency Management Agency, upon his retirement. Jamie has served as director for 13 years and during that time has provided first responders and Delaware citizens with emergency preparedness training and education to keep Delawareans safe when hazards such as hurricanes, tornadoes, and fires hit Delaware. His efforts will be a guide and inspiration for the hard-working employees at DEMA and the many first responders in Delaware for years to come.

Jamie has a lifetime of experience when it comes to responding to emergency situations. In 1970, he began his education in fire protection technology at Delaware Technical Community College. He studied the causes and proper responses to various hazards and preventive measures that can be taken to avoid them entirely. Jamie took the knowledge he gained from his education and in 1976 began working with the Delaware State Fire School as the emergency service training administrator. It was his responsibility to supervise instructors, research technical information, and work with fire, rescue, and emergency medical services to develop necessary guidelines and effective procedures.

Then, in 2000, he took on the role of executive secretary of the Delaware Volunteer Firemen's Association, where he was tasked with following legislation at every level of government that affected DVFA's membership. In this role, he researched different laws and ordinances to ensure that the DVFA was following the proper guidelines. Thanks to Jamie, Delaware's firefighters stayed informed on the regulations that were put in place to keep themselves and those in emergency situations safe.

Jamie has been a dedicated public servant for years. Before his appointment to director of DEMA, he was serving and protecting Delaware through his consistent endeavors to remain on the cutting edge of best practices in emergency protocol and then use that experience to educate others in the field. He is active in the Smyrna Little League and continues to volunteer with the Delaware Fire Service.

On behalf of Senator CHRIS COONS and Congressman JOHN CARNEY, I wholeheartedly thank Jamie Turner for his service to the State of Delaware. His model leadership and dedication has improved the quality of our State's emergency response systems and has kept countless residents safe. We offer our sincere congratulations on a job well done and wish him and his wife Debbie, their daughters Kim and Katie, husbands Mike and Sean respectively, and their grandchildren Madelyn, Harper, Keegan, and Kolton many happy years to come.●

TRIBUTE TO VAUGHN THOMAS HAWKES

● Mr. CRAPO. Mr. President, I wish to honor Vaughn Thomas Hawkes on his 80th birthday. Vaughn is a native Idahoan whose family roots in the State go back generations. He is one of nine children born to a farm family outside of Preston, where he learned hard work and ingenuity are the keys to a good life. The work ethic he learned early on has served him well through his 80 years, but he had a spirit of adventure that was unusual for an Idaho farm boy. After he finished college at Utah State University and married his sweetheart of close to 56 years, Frances Arlene Anderson, they embarked on a journey that took them to the tiny island territory of American Samoa, where he first taught high school chemistry, math, and physics, and then served as principal at Mapusaga High School. But perhaps some may think his greatest achievement during that time was that he was instrumental in introducing American football to the Samoan people—something many college and NFL teams have appreciated for many years now. An educator by training and inclination, Vaughn spent many years in administrative positions at the Blackfoot School District before finishing his career in the Provo School District where he retired.

His devotion to his faith has been manifest in many ways, including missionary service throughout the world—first as a young missionary in western Canada; then in American Samoa; then in Milan, Italy; and most recently in Santa Monica, CA. His teaching nature has been evident far beyond his professional career, as he has been given the opportunity to educate through that missionary service. Upon his retirement from education several years ago, he had served in teaching positions at the LDS Missionary Training Center and the BYU-Idaho Pathways Program—ever searching to help those who are seeking improvement in their educational pursuits.

His friends and neighbors know him as a tinkerer, a man who can fix anything. He maintains a world-class collection of tools and parts you never knew you were missing. He is the proud father of eight children—Susan, Richard, Diane, Pamela, Cynthia, Daniel, John, and Scott. His eldest daughter, Susan, has worked for me for many years, and I have had the opportunity to get to know Vaughn on a personal level. While he may count them as his greatest achievements, each one of them is grateful for his influence and support in their lives. He taught them how to work, how to fight for what is right and fair, to value education and learning, to take the adventurous path, and to be faithful to the Lord. He has built a life of service and devotion to his family, friends, and faith and serves as a tremendous example of kindness and strength to all who know him.

As a young farm boy, Vaughn had an opportunity to receive the CONGRESSIONAL RECORD every day through the mail. He was fascinated by all that transpired in Congress and read the documents studiously. It was only the beginning of a lifetime of curiosity about the world around him. So it seemed a fitting tribute to honor his 80th birthday to provide him with his own mention in that illustrious RECORD. We wish him a very happy 80th birthday.●

TRIBUTE TO WAR CHIEF JOSEPH MEDICINE CROW

● Mr. DAINES. Mr. President, I would like to wish happy birthday to the last Crow war chief, Joseph Medicine Crow, who is celebrating his 102nd birthday today. He has served proudly as the Crow Tribe's historian and storyteller, is a decorated World War II veteran, and was the first in his tribe to attain a master's degree.

Medicine Crow has lived a life filled with numerous accomplishments. He is a recipient of the Presidential Medal of Freedom. The White House identified him as both ''a warrior and living legend'' when he received the Medal of Freedom in 2009. In 2006, his personal memoir, ''Counting Coup,'' was published by National Geographic. He is considered one of the most celebrated Native American soldiers due to his selfless service in World War II.

With his great-grandmother, grandmother, mother, and uncle all living past 100 years of age, Medicine Crow credits his long life to his strong family roots. Medicine Crow's secret advice to living such a long and full life? He advises going to sleep early, sleeping 8 hours, eating breakfast, keeping busy at work, and eating healthy and generously. He also touched on the positive influences of his wife, who urged him to maintain good habits. His positive, endearing spirit and sense of humor truly keeps him young.

Medicine Crow's spirit, humility, kind disposition, and many incredible life achievements are a model for all Montanans. Happy Birthday, Chief Medicine Crow. I look forward to celebrating many more.●

TRIBUTE TO RUSTY STAFNE

● Mr. DAINES. Mr. President, I wish to recognize the loyal service of A.T. ''Rusty'' Stafne, chairman of the Fort Peck Assiniboine and Sioux Tribes. Stafne ended his term yesterday and will not be running for reelection as chairman. I am proud to honor and to congratulate him on his service and successes.

As chairman, Stafne has worked diligently for the Assiniboine and Sioux people on the Fort Peck Reservation and has held firm in his priorities. He has worked to honor veterans, specifically those who served in World War II, and has worked tirelessly to protect wildlife in Montana and on the Fort Peck Reservation.

We thank Chairman Stafne for his involvement in the Senate Indian Affairs Committee. He has been a tireless advocate for rural water projects and other challenges facing the tribes. He has traveled to Washington, DC, to testify in front of Congress and has broadened the eyes of many—giving new and better insight into the life of tribal men and women, so that we can work together to better serve and protect our tribal nations.

I am thankful for Chairman Stafne's work on behalf of the tribe. His loyalty, priorities, and hard work set an amazing example to the rest of Montana and our great Nation as a whole.●

MESSAGES FROM THE HOUSE

At 11:27 a.m., a message from the House of Representatives, delivered by Mr. Novotny, one of its reading clerks, announced that the House has passed the following bill, in which it requests the concurrence of the Senate:

H.R. 3033. An act to require the President's annual budget request to Congress each year to include a line item for the Research in Disabilities Education program of the National Science Foundation and to require the National Science Foundation to conduct research on dyslexia.

ENROLLED BILL SIGNED

The President pro tempore (Mr. HATCH) announced that on October 26, 2015, he had signed the following enrolled bill, previously signed by the Speaker of the House:

H.R. 558. An act to designate the facility of the United States Postal Service located at 55 South Pioneer Boulevard in Springboro, Ohio, as the ''Richard 'Dick' Chenault Post Office Building''.

ENROLLED BILL SIGNED

At 12:48 p.m., a message from the House of Representatives, delivered by Mr. Novotny, one of its reading clerks, announced that the Speaker has signed the following enrolled bill:

H.R. 313. An act to amend title 5, United States Code, to provide leave to any new Federal employee who is a veteran with a service-connected disability rated at 30 percent or more for purposes of undergoing medical treatment for such disability, and for other purposes.

The enrolled bill was subsequently signed by the President pro tempore (Mr. HATCH).

At 2:38 p.m., a message from the House of Representatives, delivered by Mrs. Cole, one of its reading clerks, announced that the House has passed the following bill, in which it requests the concurrence of the Senate:

H.R. 3819. An act to provide an extension of Federal-aid highway, highway safety, motor carrier safety, transit, and other programs funded out of the Highway Trust Fund, and for other purposes.

MEASURES REFERRED

The following bill was read the first and the second times by unanimous consent, and referred as indicated:

H.R. 3033. An act to require the President's annual budget request to Congress each year to include a line item for the Research in Disabilities Education program of the National Science Foundation and to require the National Science Foundation to conduct research on dyslexia; to the Committee on Health, Education, Labor, and Pensions.

ENROLLED BILLS PRESENTED

The Secretary of the Senate reported that on October 26, 2015, she had presented to the President of the United States the following enrolled bills:

S. 1362. An act to amend title XI of the Social Security Act to clarify waiver authority regarding programs of all-inclusive care for the elderly (PACE programs).

S. 2162. An act to establish a 10–year term for the service of the Librarian of Congress.

REPORTS OF COMMITTEES

The following reports of committees were submitted:

By Mr. THUNE, from the Committee on Commerce, Science, and Transportation, with an amendment in the nature of a substitute:

S. 1326. A bill to amend certain maritime programs of the Department of Transportation, and for other purposes (Rept. No. 114–158).

By Mr. CORKER, from the Committee on Foreign Relations, without amendment:

S. 1789. A bill to improve defense cooperation between the United States and the Hashemite Kingdom of Jordan.

EXECUTIVE REPORTS OF COMMITTEES

The following executive reports of nominations were submitted:

By Mr. McCAIN for the Committee on Armed Services.

Air Force nomination of Col. Thomas K. Wark, to be Brigadier General.

Air Force nomination of Col. Howard P. Purcell, to be Brigadier General.

Air Force nomination of Col. Allan L. Swartzmiller, to be Brigadier General.

Army nomination of Lt. Gen. David D. Halverson, to be Lieutenant General.

Army nomination of Maj. Gen. Kenneth R. Dahl, to be Lieutenant General.

Army nomination of Col. Erik H. Torring III, to be Brigadier General.

Army nomination of Maj. Gen. Thomas S. Vandal, to be Lieutenant General.

Army nomination of Col. Valeria Gonzalez-Kerr, to be Brigadier General.

Army nomination of Col. John J. Morris, to be Brigadier General.

Air Force nomination of Brig. Gen. Stephen E. Markovich, to be Major General.

Army nomination of Col. Marta Carcana, to be brigadier General.

Mr. McCAIN. Mr. President, for the Committee on Armed Services I report favorably the following nomination lists which were printed in the RECORDS on the dates indicated, and ask unanimous consent, to save the expense of reprinting on the Executive Calendar that these nominations lie at the Secretary's desk for the information of Senators.

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

Air Force nominations beginning with Brandon R. Abel and ending with Brandon A. Zuercher, which nominations were received by the Senate and appeared in the Congressional Record on June 24, 2015.

Air Force nominations beginning with Michelle T. Aaron and ending with Kirk P. Winger, which nominations were received by the Senate and appeared in the Congressional Record on September 9, 2015.

Air Force nominations beginning with Quentin D. Bagby and ending with Mary A. Workman, which nominations were received by the Senate and appeared in the Congressional Record on September 9, 2015.

Air Force nominations beginning with Robert H. Alexander and ending with Justin

David Wright, which nominations were received by the Senate and appeared in the Congressional Record on September 9, 2015.

Army nomination of Matthew P. Tarjick, to be Lieutenant Colonel.

Army nomination of Judith S. Meyers, to be Major.

Army nominations beginning with Thomas W. Wisenbaugh and ending with Harold P. Xenitelis, which nominations were received by the Senate and appeared in the Congressional Record on September 9, 2015.

Army nomination of Michael A. Blaine, to be Colonel.

Navy nomination of Terry A. Petropoulos, to be Lieutenant Commander .

By Mr. THUNE for the Committee on Commerce, Science, and Transportation.

*Sarah Elizabeth Feinberg, of West Virginia, to be Administrator of the Federal Railroad Administration.

*Nomination was reported with recommendation that it be confirmed subject to the nominee's commitment to respond to requests to appear and testify before any duly constituted committee of the Senate.

(Nominations without an asterisk were reported with the recommendation that they be confirmed.)

INTRODUCTION OF BILLS AND JOINT RESOLUTIONS

The following bills and joint resolutions were introduced, read the first and second times by unanimous consent, and referred as indicated:

By Mr. MENENDEZ (for himself, Mr. SCHUMER, Mrs. GILLIBRAND, and Mr. BOOKER):

S. 2207. A bill to require the Secretary of State to offer rewards of not less than $10,000,000 for information that leads to the arrest or conviction of suspects in connection with the bombing of Pan Am Flight 103; to the Committee on Foreign Relations.

By Mrs. MURRAY (for herself, Ms. BALDWIN, Mr. BLUMENTHAL, Mr. BROWN, Ms. CANTWELL, Mr. FRANKEN, Mrs. GILLIBRAND, Ms. KLOBUCHAR, Mr. LEAHY, Ms. MIKULSKI, Mr. SANDERS, Ms. HIRONO, and Mr. CASEY):

S. 2208. A bill to promote the economic security and safety of survivors of domestic violence, dating violence, sexual assault, or stalking, and for other purposes; to the Committee on Health, Education, Labor, and Pensions.

By Mr. CRAPO:

S. 2209. A bill to revise various laws that interfere with the right of the people to obtain and use firearms for all lawful purposes; to the Committee on the Judiciary.

By Mr. BLUMENTHAL (for himself, Ms. BALDWIN, and Mr. MARKEY):

S. 2210. A bill to require the Secretary of Veterans Affairs to carry out a program to establish peer specialists in patient aligned care teams at medical centers of the Department of Veterans Affairs, and for other purposes; to the Committee on Veterans' Affairs.

By Mr. MORAN (for himself and Mr. UDALL):

S. 2211. A bill to authorize additional uses of the Spectrum Relocation Fund; to the Committee on Commerce, Science, and Transportation.

ADDITIONAL COSPONSORS

S. 12

At the request of Mr. BLUNT, the name of the Senator from West Virginia (Mrs. CAPITO) was added as a cosponsor of S. 12, a bill to amend the Internal Revenue Code of 1986 to exempt employees with health coverage under TRICARE or the Veterans Administration from being taken into account for purposes of determining the employers to which the employer mandate applies under the Patient Protection and Affordable Care Act.

S. 281

At the request of Mr. BLUNT, the name of the Senator from Nebraska (Mrs. FISCHER) was added as a cosponsor of S. 281, a bill to require a Federal agency to include language in certain educational and advertising materials indicating that such materials are produced and disseminated at taxpayer expense.

S. 520

At the request of Mr. CARDIN, the name of the Senator from California (Mrs. FEINSTEIN) was added as a cosponsor of S. 520, a bill to amend the Neotropical Migratory Bird Conservation Act to reauthorize the Act.

S. 619

At the request of Mr. CARDIN, the name of the Senator from South Dakota (Mr. ROUNDS) was added as a cosponsor of S. 619, a bill to include among the principal trade negotiating objectives of the United States regarding commercial partnerships trade negotiating objectives with respect to discouraging activity that discourages, penalizes, or otherwise limits commercial relations with Israel, and for other purposes.

S. 637

At the request of Mr. CRAPO, the name of the Senator from Colorado (Mr. BENNET) was added as a cosponsor of S. 637, a bill to amend the Internal Revenue Code of 1986 to extend and modify the railroad track maintenance credit.

S. 682

At the request of Mr. TOOMEY, the name of the Senator from Arizona (Mr. FLAKE) was added as a cosponsor of S. 682, a bill to amend the Truth in Lending Act to modify the definitions of a mortgage originator and a high-cost mortgage.

S. 746

At the request of Mr. GRASSLEY, the name of the Senator from New Mexico (Mr. HEINRICH) was added as a cosponsor of S. 746, a bill to provide for the establishment of a Commission to Accelerate the End of Breast Cancer.

S. 773

At the request of Mrs. MURRAY, the name of the Senator from Maryland (Ms. MIKULSKI) was added as a cosponsor of S. 773, a bill to prevent harassment at institutions of higher education, and for other purposes.

S. 776

At the request of Mr. ROBERTS, the name of the Senator from Minnesota (Ms. KLOBUCHAR) was added as a cosponsor of S. 776, a bill to amend title XVIII of the Social Security Act to improve access to medication therapy management under part D of the Medicare program.

S. 1042

At the request of Mr. MENENDEZ, the name of the Senator from Florida (Mr. NELSON) was added as a cosponsor of S. 1042, a bill to amend the Outer Continental Shelf Lands Act to permanently prohibit the conduct of offshore drilling on the outer Continental Shelf in the Mid-Atlantic, South Atlantic, and North Atlantic planning areas.

S. 1249

At the request of Mr. MENENDEZ, the name of the Senator from Minnesota (Mr. FRANKEN) was added as a cosponsor of S. 1249, a bill to amend the Fair Credit Reporting Act to provide protections for active duty military consumers, and for other purposes.

S. 1334

At the request of Ms. MURKOWSKI, the names of the Senator from New Jersey (Mr. BOOKER) and the Senator from Louisiana (Mr. VITTER) were added as cosponsors of S. 1334, a bill to strengthen enforcement mechanisms to stop illegal, unreported, and unregulated fishing, to amend the Tuna Conventions Act of 1950 to implement the Antigua Convention, and for other purposes.

S. 1375

At the request of Mr. DURBIN, the name of the Senator from Oregon (Mr. MERKLEY) was added as a cosponsor of S. 1375, a bill to designate as wilderness certain Federal portions of the red rock canyons of the Colorado Plateau and the Great Basin Deserts in the State of Utah for the benefit of present and future generations of people in the United States.

S. 1565

At the request of Mr. REED, the name of the Senator from New Mexico (Mr. UDALL) was added as a cosponsor of S. 1565, a bill to allow the Bureau of Consumer Financial Protection to provide greater protection to servicemembers.

S. 1719

At the request of Ms. COLLINS, the name of the Senator from Alaska (Ms. MURKOWSKI) was added as a cosponsor of S. 1719, a bill to provide for the establishment and maintenance of a National Family Caregiving Strategy, and for other purposes.

S. 1937

At the request of Mr. UDALL, the name of the Senator from Maine (Mr. KING) was added as a cosponsor of S. 1937, a bill to amend the Richard B. Russell National School Lunch Act and the Child Nutrition Act of 1966 to improve nutrition in tribal areas, and for other purposes.

S. 1982

At the request of Mr. CARDIN, the names of the Senator from North Carolina (Mr. TILLIS), the Senator from Montana (Mr. DAINES), the Senator from Arizona (Mr. FLAKE) and the Senator from West Virginia (Mrs. CAPITO) were added as cosponsors of S. 1982, a bill to authorize a Wall of Remembrance as part of the Korean War Veterans Memorial and to allow certain

private contributions to fund the Wall of Remembrance.

S. 2009

At the request of Mr. WYDEN, the name of the Senator from Oregon (Mr. MERKLEY) was added as a cosponsor of S. 2009, a bill to prohibit the sale of arms to Bahrain.

S. 2042

At the request of Mrs. MURRAY, the name of the Senator from Hawaii (Mr. SCHATZ) was added as a cosponsor of S. 2042, a bill to amend the National Labor Relations Act to strengthen protections for employees wishing to advocate for improved wages, hours, or other terms or conditions of employment and to provide for stronger remedies for interference with these rights, and for other purposes.

S. 2089

At the request of Ms. CANTWELL, the name of the Senator from Rhode Island (Mr. WHITEHOUSE) was added as a cosponsor of S. 2089, a bill to provide for investment in clean energy, to empower and protect consumers, to modernize energy infrastructure, to cut pollution and waste, to invest in research and development, and for other purposes.

S. 2145

At the request of Mr. GRAHAM, the name of the Senator from New York (Mrs. GILLIBRAND) was added as a cosponsor of S. 2145, a bill to make supplemental appropriations for fiscal year 2016.

S. 2148

At the request of Mr. WYDEN, the name of the Senator from Massachusetts (Mr. MARKEY) was added as a cosponsor of S. 2148, a bill to amend title XVIII of the Social Security Act to prevent an increase in the Medicare part B premium and deductible in 2016.

S. 2152

At the request of Mr. CORKER, the names of the Senator from Arkansas (Mr. BOOZMAN) and the Senator from Michigan (Mr. PETERS) were added as cosponsors of S. 2152, a bill to establish a comprehensive United States Government policy to encourage the efforts of countries in sub-Saharan Africa to develop an appropriate mix of power solutions, including renewable energy, for more broadly distributed electricity access in order to support poverty reduction, promote development outcomes, and drive economic growth, and for other purposes.

S. 2166

At the request of Mr. BLUNT, the name of the Senator from Pennsylvania (Mr. CASEY) was added as a cosponsor of S. 2166, a bill to amend part B of title IV of the Social Security Act to ensure that mental health screenings and assessments are provided to children and youth upon entry into foster care.

S. 2184

At the request of Mr. ISAKSON, his name was added as a cosponsor of S. 2184, a bill to direct the President to establish guidelines for United States foreign development and economic assistance programs, and for other purposes.

AMENDMENT NO. 2621

At the request of Mr. WYDEN, the name of the Senator from Massachusetts (Ms. WARREN) was added as a cosponsor of amendment No. 2621 proposed to S. 754, an original bill to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

AMENDMENT NO. 2716

At the request of Mr. BURR, the names of the Senator from Wisconsin (Mr. JOHNSON), the Senator from Arizona (Mr. MCCAIN), the Senator from Delaware (Mr. CARPER), the Senator from Iowa (Mr. GRASSLEY) and the Senator from South Dakota (Mr. THUNE) were added as cosponsors of amendment No. 2716 proposed to S. 754, an original bill to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. BLUMENTHAL (for himself, Ms. BALDWIN, and Mr. MARKEY):

S. 2210. A bill to require the Secretary of Veterans Affairs to carry out a program to establish peer specialists in patient aligned care teams at medical centers of the Department of Veterans Affairs, and for other purposes; to the Committee on Veterans' Affairs.

Mr. BLUMENTHAL. Mr. President, in 2013, the VA estimated that about 1.5 million veterans required mental health services, which VA provides in a variety of settings. In addition to the traditional VA medical centers, veterans may access mental health services and support through Vet Centers—which often appeal to veterans because of their welcoming, home-like environment; Community Based Outpatient Clinics, which play an important role in telehealth delivery by connecting rural veterans to psychiatry services from the medical center home-base, a Veterans Crisis Line, VA staff on college and university campuses, and other outreach efforts. Another important means of delivering mental health services has been the inclusion of mental health professionals within primary care delivery through VA's Patient Aligned Care Teams, which improves the screening process and allows providers to recognize and treat mental health issues occurring among those veterans who present in their primary care locations.

In addition to providing ongoing care to veterans with mental health needs, VA plays a role in suicide risk assessment and prevention among veterans. According to VA, about one-quarter of the 18 to 22 veterans who die by suicide each day were receiving care through VA. Suicide rates are even higher among those veterans who do not use VA for the health care services. Given the stigma and reluctance of some veterans to seek mental health treatment, veterans using VA for primary care may be missing a key entry point to the peer support model of care. Expanding this effective model into the primary care setting could provide another opportunity for veterans to access mental health services through VA. That is why, today, I am introducing—with my cosponsors Senators BALDWIN and MARKEY—the Veteran Partners' Efforts to Enhance Reintegration, Veteran PEER Act, a bill that would expand the peer support model of care for mental health services within the VA system to help ensure that veterans receive the effective and timely care they deserve.

VA has begun a program to co-locate mental health care providers within primary care settings in an effort to promote effective treatment of common mental health conditions in the primary care environment. This is a positive step; however, the peer support model of care for mental health services has not been similarly integrated. Research on the use of the peer support model of care for mental health services within the VA has shown that Peer Specialists helped patients become more active in treatment, which can promote recovery. Peer support was recognized by the Centers for Medicare and Medicaid Services as an evidence-based practice in 2007; and over 20 states have Medicaid reimbursement for peer support services. In response to the President's August 2014 Executive Orders to improve mental health services for veterans, VA committed to integrating and expanding the peer support model of care beyond traditional mental health settings into primary care clinics in order to better connect with veterans wherever they seek care. However, progress toward placing Peer Specialists in primary care teams has been slow.

The Veteran PEER bill would require VA to expand its use of Peer Specialists—VA employees who promote veterans' recovery by sharing their own recovery stories, providing encouragement, and teaching skills needed for successful recovery. These professionals may also provide case management assistance, help with accessing the right mental health care, and teach coping and self-advocacy skills. In general, peer support programs aim to develop veterans' self-management skills and restore participation in work and other social roles. Recognizing this effective model of care, this bill would require VA to establish Peer Specialists in Patient Aligned Care Teams within VA medical centers to promote the use and integration of mental health services into the primary care setting. Over a two year period, the program would be carried out in 25 locations.

The bill directs VA to take into consideration the needs of female veterans when establishing peer support programs, ensure that female Peer Specialists are made available to veterans through the program, and consider rural and underserved areas when selecting program locations. VA would be required to regularly report to Congress on the progress of the program including on its benefits to veterans and their family members and data on the gender of clients served by the program. Given that VA is one of the largest employers of Peer Specialists, VA's regular reporting on the program would not only allow Congress to conduct appropriate oversite of the activities, but could also provide important insights for the wider peer support community.

Given the pressing need for mental health services, it is imperative that we equip VA with the resources and organizational structure it needs to care for veterans who access these services and to find ways to reach more veterans with effective mental health services when they need them. Expanding the peer support model into the primary care setting could provide another opportunity for veterans to access mental health services through VA. As a nation we have asked more of these individuals than most of us can comprehend. We must now honor the promise we made as a nation—to take care of those who have taken care of us.

Mr. President, I ask unanimous consent that the text of the bill and letters of support be printed in the RECORD.

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

S. 2210

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Veteran Partners' Efforts to Enhance Reintegration Act'' or the ''Veteran PEER Act''.

SEC. 2. PROGRAM ON ESTABLISHMENT OF PEER SPECIALISTS IN PATIENT ALIGNED CARE TEAM SETTINGS WITHIN MEDICAL CENTERS OF DEPARTMENT OF VETERANS AFFAIRS.

(a) PROGRAM REQUIRED.—The Secretary of Veterans Affairs shall carry out a program to establish peer specialists in patient aligned care teams at medical centers of the Department of Veterans Affairs to promote the use and integration of mental health services in a primary care setting.

(b) TIMEFRAME FOR ESTABLISHMENT OF PROGRAM.—The Secretary shall carry out the program at medical centers of the Department as follows:

(1) Not later than 180 days after the date of the enactment of this Act, at not fewer than ten medical centers of the Department.

(2) Not later than two years after the date of the enactment of this Act, at not fewer than 25 medical centers of the Department.

(c) SELECTION OF LOCATIONS.—

(1) IN GENERAL.—The Secretary shall select medical centers for the program as follows:

(A) Not fewer than five shall be medical centers of the Department that are designated by the Secretary as polytrauma centers.

(B) Not fewer than ten shall be medical centers of the Department that are not designated by the Secretary as polytrauma centers.

(2) CONSIDERATIONS.—In selecting medical centers for the program under paragraph (1), the Secretary shall consider the feasibility and advisability of selecting medical centers in the following areas:

(A) Rural areas and other areas that are underserved by the Department.

(B) Areas that are not in close proximity to an active duty military installation.

(C) Areas representing different geographic locations, such as census tracts established by the Bureau of the Census.

(d) GENDER-SPECIFIC SERVICES.—In carrying out the program at each location selected under subsection (c), the Secretary shall ensure that—

(1) the needs of female veterans are specifically considered and addressed; and

(2) female peer specialists are included in the program.

(e) REPORTS.—

(1) PERIODIC REPORTS.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and not less frequently than once every 180 days thereafter until the Secretary determines that the program is being carried out at the last location to be selected under subsection (c), the Secretary shall submit to Congress a report on the program.

(B) ELEMENTS.—Each report required by subparagraph (A) shall include the following:

(i) The findings and conclusions of the Secretary with respect to the program during the 180-day period preceding the submittal of the report.

(ii) An assessment of the benefits of the program to veterans and family members of veterans during the 180-day period preceding the submittal of the report.

(2) FINAL REPORT.—Not later than 180 days after the Secretary determines that the program is being carried out at the last location to be selected under subsection (c), the Secretary shall submit to Congress a report detailing the recommendations of the Secretary as to the feasibility and advisability of expanding the program to additional locations.

Chicago, IL, October 14, 2015.

Hon. RICHARD BLUMENTHAL,
U.S. Senate,
Washington, DC.

DEAR SENATOR BLUMENTHAL: On behalf of the Depression and Bipolar Support Alliance (DBSA), it is with great pleasure that I endorse the Veteran Partners' Efforts to Enhance Re-integration (PEER) Act. This bill addresses a critically important gap within the U.S. Department of Veterans Affairs (VA) that inhibits access to behavioral health services. We look forward to working with you to improve veterans' access to care.

Since 2013, the VA has effectively used peer support specialists to enhance behavioral health care delivered to veterans in behavioral health settings. Yet, a majority of veterans in need of behavioral health care will enter the VA system through a primary care center. To help create the necessary connection from primary care to behavioral health services, the PEER Act will utilize behavioral health peer support specialists to assist veterans in various primary care settings.

Specifically, the bill will require the VA to establish a pilot program to assess the feasibility and advisability of establishing peer support specialists in Patient Aligned Care Teams within VA medical centers to promote the use and integration of mental health services into the primary care setting. DBSA strongly supports the requirement that VA medical centers give special consideration to the needs of female veterans when designing the pilot programs and ensure that female peer support specialists are available in each of the pilot locations. We also welcome the collection and reporting of data that will provided to Congress every six months from the pilot. The VA utilizes the largest number of peer support specialists in the nation. As such, this data will help improve the role of the peer support specialists within the VA and throughout America's entire health care system.

As the leading peer-led organization supporting individuals with mood disorders and their families, DBSA understands the importance of peer support for individuals with a behavioral health condition. We feel strongly that expanded use of peer specialists within the VA will increase veteran engagement in their care, and lead to better outcomes and sustained wellness. We applaud you for leading this new effort and stand ready to support the VA as it implements this pilot program.

Sincerely,

ALLEN DOEDERLEIN,
President,
Depression and Bipolar Support Alliance.

NATIONAL ALLIANCE ON MENTAL ILLNESS,
Arlington, VA, October 26, 2015.

Hon. RICHARD BLUMENTHAL,
U.S. Senate,
Washington, DC.

DEAR SENATOR BLUMENTHAL: On behalf of the National Alliance on Mental Illness (NAMI), I am writing to offer our strong support for your proposed legislation, the Veteran Partners' Efforts to Enhance Re-Integration (PEER) Act. As the nation's largest organization representing people living with serious mental illness and their families, NAMI is pleased to support this important legislation.

As you know, the Department of Veterans Affairs (VA) currently uses Peer Specialists to assist veterans living with mental illness. These Peer Specialists do a tremendous job in helping veterans' access mental health services and navigate the complicated VA health care system. Every day they promote recovery through development of self-management skills and assistance in moving toward employment and community integration.

Your PEER bill would direct the VA to establish a pilot program to assess the feasibility of ''going to scale'' in the VA with a peer support program built on Patient Aligned Care Teams within VA medical centers across the nation. This would be a major step forward in promoting integration of mental health services into primary care settings. Your bill would also direct the VA to specifically take into consideration the needs of female veterans when designing pilot programs and to ensure that female peer support specialists are available in each of the pilot locations.

NAMI strongly supports this effort to expand access to peer specialists in the VA. Thank you for bringing this important legislation forward. NAMI looks forward to working with you to ensure its swift passage.

Sincerely,

MARY GILIBERTI.

MILITARY OFFICERS ASSOCIATION OF AMERICA
Alexandria, VA, October 26, 2015.

Hon. RICHARD BLUMENTHAL,
Ranking Member, Committee on Veterans Affairs, U.S. Senate, Washington, DC.

DEAR SENATOR BLUMENTHAL: On behalf of the more than 390,000 members of the Military Officers Association of America

(MOAA), I'm writing to thank you for sponsoring the ''Veteran Partners Efforts to Enhance Reintegration (PEER) Act,'' a bill that would establish a two-year pilot program that requires the Department of Veterans Affairs to establish peer specialists in patient aligned care teams at 25 medical center locations.

MOAA has long supported peer support programs as a means to enhance delivery of health care services. By extending VA's existing mental health peer support model into the primary care setting helps to further reduce barriers in accessing mental health services while also supporting the Department's current efforts at integrating mental-physical health care concurrently to increase system capacity.

All veterans deserve access to mental health care when they need it and wherever they may live. As such, we are particularly grateful for special consideration in this legislation for female veterans and those living in rural or underserved areas.

I greatly appreciate your leadership and look forward to the passage of this timely legislation.

Sincerely,

NORBERT RYAN, Jr.,
President.

AMERICAN PUBLIC HEALTH ASSOCIATION,
October 23, 2015.

Hon. RICHARD BLUMENTHAL,
Ranking Member, Senate Committee on Veterans' Affairs, Washington, DC.

DEAR RANKING MEMBER BLUMENTHAL: On behalf of the American Public Health Association, a diverse community of public health professionals who champion the health of all people and communities, I write in support of the Veteran Partners' Efforts to Enhance Reintegration Act, which would require the inclusion of peer support specialists in Patient Aligned Care Teams within medical centers at the Department of Veterans Affairs.

Rates of mental illness are disproportionately high among U.S. veterans, particularly posttraumatic stress disorder, substance abuse disorders, depression, anxiety and military sexual trauma. Nearly 50 percent of combat veterans from Iraq report that they have suffered from PTSD, and close to 40 percent of these same veterans report problem alcohol use. In 2010, about 22 veterans died each day as a result of suicide. Military culture promotes inner strength, self-reliance and the ability to shake off injury, which may contribute to stigma surrounding mental health issues. Stigma may create a reluctance to seek help and a fear of negative social consequences, and is the most often cited reason for why people to do not seek counseling or other mental health services.

Through a peer support model of care, Peer Specialists—veterans who have recovered or are recovering from a mental health condition—provide veterans with assistance in accessing mental health services, navigating the health care system and skills needed for a successful recovery. Expanding the peer support model to the primary care setting may offer a key entry point for those reluctant to access mental health services. The bill would also direct the VA to take into consideration the needs of female veterans and locations that are underserved.

Thank you for your commitment to the health and wellbeing of U.S. veterans and to improving access to mental health services within the VA.

Sincerely,

GEORGES C. BENJAMIN, MD,
Executive Director.

AMENDMENTS SUBMITTED AND PROPOSED

SA 2749. Mr. BURR (for himself and Mrs. FEINSTEIN) proposed an amendment to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

TEXT OF AMENDMENTS

SA 2749. Mr. BURR (for himself and Mrs. FEINSTEIN) proposed an amendment to amendment SA 2716 proposed by Mr. BURR (for himself and Mrs. FEINSTEIN) to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; as follows:

On page 11, line 3, strike ''period'' and insert ''periodic''.

On page 11, line 10, strike ''532'' and insert ''632''.

On page 20, line 21, strike ''measures'' and insert ''measure''.

On page 56, line 8, strike ''and'' and all that follows through ''(7)'' on line 9 and insert the following:

(7) the term ''national security system'' has the meaning given the term in section 11103 of title 40, United States Code; and

(8)

On page 57, line 8, strike ''and''.

On page 57, line 11, strike the period at the end and insert ''; and''.

On page 57, between lines 11 and 12, insert the following:

''(4) the term 'national security system' has the meaning given the term in section 11103 of title 40, United States Code.

On page 64, lines 14 and 15, strike ''Notwithstanding section 202, in this subsection'' and insert ''In this subsection only''.

On page 69, line 13, strike ''all taken'' and insert ''taken all''.

On page 76, line 22, insert ''and the Director of the Office of Management and Budget'' after ''Intelligence''.

On page 77, lines 12 and 13, strike '', as defined in section 11103 of title 40, United States Code''.

On page 77, line 14, insert ''and the Director of the Office of Management and Budget'' after ''Intelligence''.

On page 78, between lines 2 and 3, insert the following:

(d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to designate an information system as a national security system.

On page 78, line 18, strike ''owned'' and insert ''used''.

Beginning on page 80, line 25, strike ''use'' and all that follows through ''other'' on page 81, line 6, and insert ''intrusion detection and prevention capabilities under section 230(b)(1) of the Homeland Security Act of 2002 for the purpose of ensuring the security of''.

On page 84, line 25, strike ''Act'' and insert ''Act of 2015''.

On page 85, between lines 11 and 12, insert the following:

(D) the Committee on Commerce, Science, and Transportation of the Senate;

On page 86, line 26, insert ''the Director of the National Institute of Standards and Technology and'' after ''coordination with''.

On page 88, line 8, strike ''non-civilian'' and insert ''noncivilian''.

On page 89, line 23, insert '', the Director of the National Institute of Standards and Technology,'' after ''Director''.

On page 91, line 11, strike ''203 and 204'' and insert ''303 and 304''.

On page 91, line 21, insert '', in consultation with the Director of the National Institute of Standards and Technology,'' after ''Security''.

On page 92, line 9, insert '', in consultation with the Director of the National Institute of Standards and Technology,'' after ''Secretary''.

On page 96, line 19, strike ''likely,'' and insert ''likely''.

On page 96, line 22, strike ''present'' and insert ''present,''.

Beginning on page 103, strike line 10 and all that follows through page 105, line 24, and insert the following:

(1) IN GENERAL.—Not later than 60 days after the date of enactment of this Act, the Secretary, in consultation with the Director of the National Institute of Standards and Technology and the Secretary of Homeland Security, shall convene health care industry stakeholders, cybersecurity experts, and any Federal agencies or entities the Secretary determines appropriate to establish a task force to—

(A) analyze how industries, other than the health care industry, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries;

(B) analyze challenges and barriers private entities (notwithstanding section 102(15)(B), excluding any State, tribal, or local government) in the health care industry face securing themselves against cyber attacks;

(C) review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record;

(D) provide the Secretary with information to disseminate to health care industry stakeholders for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the health care industry;

(E) establish a plan for creating a single system for the Federal Government to share information on actionable intelligence regarding cybersecurity threats to the health care industry in near real time, requiring no fee to the recipients of such information, including which Federal agency or other entity may be best suited to be the central conduit to facilitate the sharing of such information; and

(F) report to Congress on the findings and recommendations of the task force regarding carrying out subparagraphs (A) through (E).

(2) TERMINATION.—The task force established under this subsection shall terminate on the date that is 1 year after the date of enactment of this Act.

(3) DISSEMINATION.—Not later than 60 days after the termination of the task force established under this subsection, the Secretary shall disseminate the information described in paragraph (1)(D) to health care industry stakeholders in accordance with such paragraph.

(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to limit the antitrust exemption under section 104(e) or the protection from liability under section 106.

(e) CYBERSECURITY FRAMEWORK.—

(1) IN GENERAL.—The Secretary shall establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, the National Institute of Standards and Technology, and any Federal agency or entity the Secretary determines appropriate, a single, voluntary, national health-specific cybersecurity framework that—

(A) establishes a common set of voluntary, consensus-based, and industry-led standards, security practices, guidelines, methodologies, procedures, and processes that serve as

a resource for cost-effectively reducing cybersecurity risks for a range of health care organizations;

(B) supports voluntary adoption and implementation efforts to improve safeguards to address cybersecurity threats;

(C) is consistent with the security and privacy regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note) and with the Health Information Technology for Economic and Clinical Health Act (title XIII of division A, and title IV of division B, of Public Law 111–5), and the amendments made by such Act; and

(D) is updated on a regular basis and applicable to the range of health care organizations described in subparagraph (A).

(2) LIMITATION.—Nothing in this subsection shall be interpreted as granting the Secretary authority to—

(A) provide for audits to ensure that health care organizations are in compliance with the voluntary framework under this subsection; or

(B) mandate, direct, or condition the award of any Federal grant, contract, or purchase on compliance with such voluntary framework.

(3) NO LIABILITY FOR NONPARTICIPATION.—Nothing in this title shall be construed to subject a health care organization to liability for choosing not to engage in the voluntary activities authorized under this subsection.

On page 107, line 10, strike ''shall each'' and insert ''shall''.

On page 107, lines 11 and 12, strike ''each Comptroller General of the United States and''.

On page 110, strikes lines 6 through 16.

On page 111, lines 8 and 9, strike ''under subsection (b)'' and insert ''pursuant to section 9(a) of Executive Order 13636 of February 12, 2013 (78 Fed. Reg. 11742), relating to identification of critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security''.

On page 111, strike lines 22 through 24 and insert the following:

Resources of the Senate;

(F) the Committee on Energy and Commerce of the House of Representatives; and

(G) the Committee on Commerce, Science, and Transportation of the Senate.

On page 112, line 3, add a period at the end.

On page 112, strike lines 4 through 10.

On page 113, line 14, strike ''intrusion''.

Beginning on page 114, strike line 7 and all that follows through page 115, line 9.

On page 115, after line 9, add the following:

SEC. 408. STOPPING THE FRAUDULENT SALE OF FINANCIAL INFORMATION OF PEOPLE OF THE UNITED STATES.

Section 1029(h) of title 18, United States Code, is amended by striking ''title if—'' and all that follows through ''therefrom.'' and inserting ''title if the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity organized under the laws of the United States, or any State, the District of Columbia, or other Territory of the United States.''.

AUTHORITY FOR COMMITTEES TO MEET

COMMITTEE ON ARMED SERVICES

Mr. BLUNT. Mr. President, I ask unanimous consent that the Committee on Armed Services be authorized to meet during the session of the Senate on October 27, 2015, 9 a.m.

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

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

Mr. BLUNT. Mr. President, I ask unanimous consent that the Committee on Commerce, Science, and Transportation be authorized to meet during the session of the Senate on October 27, 2015, at 4 p.m., in room S–207 of the Capitol.

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

COMMITTEE ON ENERGY AND NATURAL RESOURCES

Mr. BLUNT. Mr. President, I ask unanimous consent that the Committee on Energy and Natural Resources be authorized to meet during the session of the Senate on October 27, 2015, at 9 a.m., in room SD–366 of the Dirksen Senate Office Building.

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

COMMITTEE ON FINANCE

Mr. BLUNT. Mr. President, I ask unanimous consent that the Committee on Finance be authorized to meet during the session of the Senate on October 27, 2015, at 9 a.m., in room SD–215 of the Dirksen Senate Office Building, to conduct a hearing entitled ''The Internal Revenue Service's Response to Committee Recommendations Contained in its August 5, 2015 Report.''

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

COMMITTEE ON FOREIGN RELATIONS

Mr. BLUNT. Mr. President, I ask unanimous consent that the Committee on Foreign Relations be authorized to meet during the session of the Senate on October 27, 2015, at 10 a.m.

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

SELECT COMMITTEE ON INTELLIGENCE

Mr. BLUNT. Mr. President, I ask unanimous consent that the Select Committee on Intelligence be authorized to meet during the session of the Senate on October 27, 2015, at 2 p.m.

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

PRIVILEGES OF THE FLOOR

Mr. REED. Mr. President, I ask unanimous consent that Jeremy Kuester, a fellow in my office, be granted privileges of the floor for the remainder of the session.

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

ORDERS FOR WEDNESDAY, OCTOBER 28, 2015

Mr. MCCONNELL. Mr. President, I ask unanimous consent that when the Senate completes its business today, it adjourn until 10 a.m. on Wednesday, October 28; that following the prayer and pledge, the morning hour be deemed expired, the Journal of proceedings be approved to date, and the time for the two leaders be reserved for their use later in the day; that following leader remarks, the Senate be in a period of morning business until 12 noon, with Senators permitted to speak therein for up to 10 minutes each.

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

ADJOURNMENT UNTIL 10 A.M. TOMORROW

Mr. MCCONNELL. Mr. President, if there is no further business to come before the Senate, I ask unanimous consent that it stand adjourned under the previous order.

There being no objection, the Senate, at 6:23 p.m., adjourned until Wednesday, October 28, 2015, at 10 a.m.