enforcement of laws. Throughout this Congress, my Republican colleagues often rail against the Federal Government telling State and local governments what to do, but now when it comes to something as important as public safety and law enforcement, it is suddenly OK to second guess State and local law enforcement?

Instead of turning hard-working immigrants into bogeymen, we should be focusing on real solutions for violent crime in our communities. If my colleagues who support this bill are serious about addressing violence in America, then they should come to the table to talk about how we can strengthen our laws to keep guns out of the hands of criminals and the mentally ill.

I have been saying, along with many of my colleagues for over a year now, if my Republican colleagues want to discuss immigration reform, we welcome that debate. Everyone agrees our immigration system is broken and needs reform. It has been 28 months since the Senate passed a comprehensive immigration bill that had strong bipartisan support.

Even though it was not perfect from my perspective, we nonetheless worked together to come up with a compromise bill, but House Republicans ducked the issue and refused to take up the immigration reform bill. The Senate comprehensive immigration bill would have reduced the Federal deficit by $1 trillion in just two decades because of the broad economic benefits immigration reform granted.

It would have protected and united families, strengthened our border security, improved our economy, and encouraged job creation in our country. The Senate's bill would have gotten millions of people out of the shadows, requiring them to pass criminal background checks and earn their path to citizenship. It would have let immigration enforcement officials focus on true security threats to our country.

The Senate's immigration bill included $46 billion in new resources to help our Border Patrol, Immigration and Customs Enforcement agents. Of this amount, roughly $30 billion was added to the bill to further secure our borders, but that is not enough for some Republicans. Apparently, some will not be happy until we literally round up every undocumented immigrant—some 11 million of them in our country—and deport them, which would be catastrophic to our economy, not to mention impossible to do. The current sanctuary cities debate is not the first time some have tried to use myths about immigrants to scare Americans. This rhetoric could not be further from the truth about immigrants.

I urge my colleagues to oppose these scare tactics and to vote no on the motion to proceed to S. 2146.

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 12:48 p.m., recessed until 2:15 p.m. and reassembled when called to order by the Presiding Officer (Mr. CORKER).

STOP SANCTUARY POLICIES AND PROTECT AMERICANS ACT—MOTION TO PROCEED—Continued

CLOTURE MOTION

The PRESIDING OFFICER. Pursuant to rule XXII, the Chair lays before the Senate the pending cloture motion, which the clerk will state.

The senior assistant legislative clerk read as follows:

CLOTURE MOTION

We, the undersigned Senators, in accordance with the provisions of rule XXII of the Standing Rules of the Senate, do hereby move to bring to a close debate on the motion to proceed to Calendar No. 252, S. 2146, a bill to hold sanctuary jurisdictions accountable for defying Federal law, to increase penalties for individuals who illegally reenter the United States after being removed, and to provide liability protection for State and local law enforcement who cooperate with Federal law enforcement and for other purposes.

Mitch McConnell, David Vitter, John Barrasso, Dan Sullivan, David Perdue, Bill Cassidy, Ron Johnson, Steve Daines, James Lankford, James E. Risch, John Boozman, Mike Lee, Richard C. Shelby, John Cornyn, Jeff Sessions, Johnny Isakson, Patrick J. Toomey.

The PRESIDING OFFICER (Mr. PORTMAN). By unanimous consent the mandatory quorum call has been waived.

The question is, Is it the sense of the Senate that debate on the motion to proceed to S. 2146, a bill to hold sanctuary jurisdictions accountable for defying Federal law, to increase penalties for individuals who illegally reenter the United States after being removed, and to provide liability protection for State and local law enforcement who cooperate with Federal law enforcement and for other purposes, shall be brought to a close?

The yeas and nays are mandatory under the rule.

The clerk will call the roll.

The senior assistant legislative clerk called the roll.

Mr. CORNYN. The following Senator is necessarily absent: the Senator from South Carolina (Mr. GRAHAM).

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

The yeas and nays resulted—yeas 54, nays 45, as follows:

[Rollcall Vote No. 280 Leg.]

YEAS—54

Alexander	Capito	Cornyn
Ayotte	Cassidy	Cotton
Barrasso	Coats	Crapo
Blunt	Cochran	Cruz
Boozman	Collins	Daines
Burr	Corker	Donnelly
Enzi	Lankford	Rounds
Ernst	Lee	Rubio
Fischer	Manchin	Sasse
Flake	McCain	Scott
Gardner	McConnell	Sessions
Grassley	Moran	Shelby
Hatch	Murkowski	Sullivan
Heller	Paul	Thune
Hoeven	Perdue	Tillis
Inhofe	Portman	Toomey
Isakson	Risch	Vitter
Johnson	Roberts	Wicker

NAYS—45

Baldwin	Heinrich	Nelson
Bennet	Heitkamp	Peters
Blumenthal	Hirono	Reed
Booker	Kaine	Reid
Boxer	King	Sanders
Brown	Kirk	Schatz
Cantwell	Klobuchar	Schumer
Cardin	Leahy	Shaheen
Carper	Markey	Stabenow
Casey	McCaskill	Tester
Coons	Menendez	Udall
Durbin	Merkley	Warner
Feinstein	Mikulski	Warren
Franken	Murphy	Whitehouse
Gillibrand	Murray	Wyden

NOT VOTING—1

Graham

The PRESIDING OFFICER. On this vote, the yeas are 54, the nays are 45.

Three-fifths of the Senators duly chosen and sworn not having voted in the affirmative, the motion is rejected.

The Senator from Florida.

UNANIMOUS CONSENT REQUEST—S. 1082

Mr. RUBIO. Mr. President, I don't think any of us in any of the 50 States have not had calls from our constituents about the Veterans' Administration. I know that certainly in Florida, I have. We are blessed to have so many people who are either in uniform or have served in uniform.

We make two fundamental promises to the men and women who serve our country. The first is that if we ever put them into hostility, they will be better equipped, better trained, and have more information than their adversaries. I, of course, fear that all three of those promises have eroded.

Here is the second promise we make to them: After they take care of us and they come home, we will take care of them. That is a promise that, sadly, is also not being kept.

There are a lot of different issues we can get into when it comes to veterans and what they are facing in this country, but one that has received a lot of attention is the Veterans' Administration and in particular the role it plays in providing health care for those returning or those who have served our country and have been facing challenges ever since. We have all had the phone calls to our office, and we have seen the media reports about it.

I am proud that last year we were able to pass legislation that gave the Secretary of the VA the ability to fire senior executives who weren't doing their jobs. This is the point—and this is where I always stop and remind everyone there are really good people working in the VA. In fact, the enormous majority of people at the VA are good people who care passionately about our veterans. There are some phenomenal VA facilities in this country, and then there are some facilities

that aren't working. There are some individuals within that agency who, quite frankly, are not doing their jobs well. The problem is that they can't be held accountable because they are protected by law, and as a result they can't be removed.

We expanded that law a year ago to include the ability to fire senior executives who weren't doing their jobs, but to date that has not been used to much effect. So earlier this year we introduced followup legislation, and the followup legislation gives the Secretary of the Department the authority to remove any employee of Veterans Affairs based on performance—or lack thereof—or misconduct. It gives them the authority to remove such individuals from the civil service or demote the individual through a reduction in grade or annual pay rate.

I am proud that this bill has gone through the process here in the Senate. It has passed out of committee and is now ready for action. I hope we will take action on this. There is a different version in the House. It has also gone through their committees, and they are waiting for their process to move it through. There are some differences between the two, which, of course, would be worked out in conference.

I think the prudent thing to do at this point, given the fact that the Senate bill has worked its way through the process and is now ready for action, is to take action. This is about creating accountability. By the way, this is about taking care of our veterans, but it is also about taking care of the people at the VA who are doing their jobs. This is also about them. It isn't fair to them that people who aren't doing their jobs continue in their positions and in many instances are increasing the workload on others because they are not performing or carrying their weight.

That is why I ask unanimous consent that the Senate proceed to the immediate consideration of Calendar No. 272, S. 1082; further, that the committee-reported amendments be agreed to, the bill, as amended, be read a third time and passed, and that the motion to reconsider be considered made and laid upon the table.

The PRESIDING OFFICER. Is there objection?

The Senator from Connecticut.

Mr. BLUMENTHAL. Mr. President, reserving the right to object, I respect deeply and in fact support the arguments made by my colleague from Florida. There are goals here to be served, and I strongly support them as well. Accountability has been lacking for too long in the Department of Veterans Affairs. That is a simple fact on which we can all agree. In fact, we took a major step in the right direction with the passage of the access and accountability act during the last session with bipartisan support.

I would support this measure if a number of simple changes were made to it to comply with the Constitution. This measure lacks some of the basic constitutional guarantees that again and again the Supreme Court of the United States has said are absolutely mandatory. This bill, unfortunately, fails to provide sufficient notice in advance of any firing or disciplinary action, a statement of cause, a right to be heard, and an opportunity for basic administrative constitutional guarantees.

I commit to work with my colleague from Florida on seeking to improve this bill. In fact, I have proposed a measure that is now pending in the Committee on Veterans' Affairs, S. 1856, which will improve the management of the VA in many of the same ways, but it avoids these constitutional pitfalls.

As a former attorney general, I care deeply about enforcement, which is to say effective enforcement. A disciplinary action now under appeal in the Federal circuit will decide the constitutionality of exactly these procedures. In the meantime, we ought to avoid creating unnecessary litigation and challenge to a law that should be enforced effectively. This one, unfortunately, cannot be. I believe strongly there are measures and ways to achieve greater accountability. It isn't a luxury or convenience; it is a necessity that the VA is held accountable. The more effective way to hold the VA accountable is to pass a measure that is fully constitutional and, in addition, provides more effective protection for whistleblowers. They are the ones who come forward speaking truth to power. They are the ones with critical facts necessary for accountability. This measure, unfortunately, fails to afford sufficient protection for those whistleblowers. Therefore, I object.

The PRESIDING OFFICER. Objection is heard.

The Senator from Florida.

Mr. RUBIO. Mr. President, the difference between this bill and the one in the House is the Whistleblower Protection Act. So if that is the issue the Senator is concerned with, I would ask if the Senator from Connecticut would then be willing not to object, to lift the objection, if we could move forward on the House bill that is now here and ready for us to take up as well because it does contain the whistleblower protection language.

The PRESIDING OFFICER. The Senator from Connecticut.

Mr. BLUMENTHAL. Mr. President, I would be more than willing—indeed, happy—to work with my colleague from Florida on specific language that improves the whistleblower protection language. I think his bill takes a step in the right direction by providing that the Office of Special Counsel provide approval for any disciplinary action. That is a good step, but I believe it could be made more effective. I think the opportunity to be heard with notice for cause or discipline or firing is essential to effective enforcement. I share the goal—strongly share it—of making sure that accountability is enforced.

The PRESIDING OFFICER. The Senator from Florida.

Mr. RUBIO. Again, the House version of this bill, which is ready for us to take up today, has stronger accountability language which we do not oppose. It simply was not included for purposes of time at the committee level. But we are prepared to move now, if we could, because the House version is here and ready for action on our part, and it has the stronger accountability language. It sounds as though, no matter what, we are probably going to have a delay here on acting on this matter.

I would say this for people watching here in the Gallery or at home or anywhere they might see it later—I just want everybody to understand what we are saying here. All we are saying in this bill is that if you work for the VA and you aren't doing your job, they get to fire you. I think people are shocked that doesn't actually exist in the entire government since there is no other job in the country where, if you don't do your job, you don't get fired. But in this instance, we are just limiting it to one agency. This should actually be the rule in the entire government. If you are not doing your job, you should get fired. But this is just limiting it to the VA because we have a crisis there with the lack of accountability.

I would hope we can move forward on this, and I am prepared to listen to anyone who wants to improve this. We went through the normal course and process in the Senate. We went through the committee. It had hearings. Opportunities for amendments were offered at the time. So if there is a good-faith effort—and I believe that there is—then let's improve this and take action on it. We need to have a VA that is more interested in the welfare and security of our veterans than the job security of Federal employees.

I said at the outset that there are really good people at the VA. The vast majority of employees at the VA are doing their jobs and doing them well. They care about these veterans. It isn't fair to them that there are people on the payroll taking up seats, taking up slots, taking up money, and taking up time who aren't doing their jobs, and they literally cannot be fired. They literally cannot be removed. It is a near impossibility. The process is so expensive, so long, so troublesome, so complicated that in essence they cannot be removed.

Unfortunately, we will not be able to move forward on this today, it appears, but I hope that in quick succession we will be able to come together and get this done to provide a higher level of accountability that is so necessary in every agency of government but none more so than Veterans Affairs.

I yield the floor.

The PRESIDING OFFICER. The Senator from Connecticut.

Mr. BLUMENTHAL. Mr. President, one last word. I want to simply concur

in the very powerful and eloquent statements made by my colleague from Florida. I think we all share those sentiments in this body that—and I am quoting now from legislation: Any employee who engages in malfeasance, overprescription of medication, insubordination, violation of any duty of care should be disciplined and very possibly fired.

We are talking about the process to achieve that end. I can commit that I will work with my colleague from Florida to make sure this body approves a measure that is effective as a deterrent to those kinds of violations of basic duty. To be effective as a deterrent, it has to be enforceable, and that is our common goal here.

The PRESIDING OFFICER. The Senator from Texas.

Mr. CORNYN. Mr. President, a few moments ago the Senate refused to move forward on an important piece of legislation, sometimes called the sanctuary cities bill. I want to explain for whoever may be listening and particularly for my colleagues what a terrible mistake our Democratic colleagues made—with the exception of two—by voting to block consideration of this piece of legislation.

What this bill would do is withhold Federal funds from jurisdictions that basically violate current law—that violate the information-sharing requirement in immigration law, Section 642 of the 1996 Illegal Immigration Reform and Immigrant Responsibility Act. Secondly, it would withhold Federal funds from those jurisdictions that refuse to honor the lawful, legal process known as the detainer, or request to notify Federal authorities if local law enforcement decides to release an illegal immigrant who happens to have been arrested for some other unrelated reason.

This is a truly important issue. As we have seen from the news, Kate Steinle out in California was killed by somebody who had repeatedly violated our laws not only by entering the country illegally but also by committing offenses against the persons and property of American citizens. Essentially what happens is when local jurisdictions give up and refuse to honor the detainers or give notice to Federal authorities before they release individuals, then people are going to get hurt. The Kate Steinles of the world will get killed.

In my State of Texas, we have had Houston police officers and other law enforcement personnel killed by illegal immigrants who have routinely broken our laws and have terrible criminal records. But if we can't get the cooperation of local law enforcement authorities to work with the Federal authorities, then unfortunately public safety will be harmed.

I am going to pull back a little bit and ask my colleagues to look at this perhaps from 30,000 feet. There is a reason at the time our Constitution was written that article VI, clause 2 simply said the Federal law is the supreme law of the land. In other words, Federal laws trump State laws and local laws.

If we think about it, as James Madison said, if we didn't have Federal law as the supreme law of the land, essentially the authority of the whole country—the elected officials, the President, the Congress, those serving in the Federal Government—the laws of the country would be made subordinate to the parts of the country—the cities, the counties, the States—that essentially defy Federal law, and our system would be in chaos.

Indeed, what our colleagues across the aisle appear to have ratified here is not one Nation under the law, but a confederation of different jurisdictions that can pick and choose what laws they want to comply with. That is a recipe for chaos.

One of the reasons I think the American people are so angry with what they see happening in Washington these days—indeed, I think they have moved beyond anger to fear. They are fearful for the future of our country. When we see individual cities and States effectively nullify Federal law by refusing to cooperate or saying: We don't care what the Federal Government says; we are going to impose our own will, this is a recipe for chaos and for the very fabric of our country to unravel.

At different points in our Nation's history we have had States which said: We aren't going to respect Federal law; we are going to nullify it, in effect. That is what these cities that defy the Federal authorities and the supremacy of Federal law are doing. They are saying we don't have to comply with the law, and so the American people—I think out of apprehension over what they see happening here when States, cities, and other jurisdictions decide to pick and choose which laws will apply—realize this is a recipe for disunity and, in this case, for danger.

The people whom we are fighting for are families and communities that want to live in peace and safety in their local communities. That is what this legislation is about. This legislation, of course, is called Stop Sanctuary Policies and Protect Americans Act. All it does, simply stated, is to restore law and order across the country and to hold certain cities that want to defy Federal law accountable. It would limit Federal funding for State and local governments that refuse to cooperate. Basically, the Stop Sanctuary Policies and Protect Americans Act encourages compliance with Federal law, as I said a moment ago, and uses the power of the purse to withhold Federal funds from those jurisdictions that refuse to cooperate with the Federal law. The goal, as I said, is to protect our communities from those who would pose a danger to our society. It does not target legal immigrants who seek to live a law-abiding and productive life here.

Frankly, I do not understand the Democrats'—with the exception of two who voted to get on this legislation and offer amendments and constructive suggestions—refusal to move this legislation forward, because it harms the public safety and it causes our country to become a confederation of different jurisdictions that can pick and choose which laws they want to enforce.

I mentioned one terrible incident over the summer, the murder of Kate Steinle in San Francisco by an illegal immigrant with a known and lengthy criminal record. This is just one example. This sad story poignantly demonstrates the consequences of the administration's abject failure when it comes to enforcing our immigration laws. People get hurt. People get killed. This legislation would address the root cause of this tragedy by targeting criminal aliens and those local entities that refuse to do anything to help the Kate Steinles of the world, and it would specifically serve to counter the policies of those city governments, such as San Francisco, that are known to shield criminal aliens from deportation. They openly defy the 1996 Federal law that requires information sharing. They openly refuse to cooperate with Federal orders and detainers and to notify the Federal Government when people are released from their jail sentence even though they know there is an outstanding deportation order pending.

This bill also extends the mandatory minimum sentence for those who attempt to reenter the country after being removed for breaking our laws. Time and again we are met with the tragic news of some other American citizen who was killed, injured or assaulted by somebody who has reentered the country, after being removed for violating our laws, and keeps coming back and committing other criminal acts.

We need to send a clear signal to those who attempt to enter our country illegally and violate and ignore our laws that they will have to answer for them and certainly will not be allowed to come back.

Some have rightly noted that this bill is not about immigration reform, and I agree. This bill is simply about enforcing our current law and holding those jurisdictions that refuse to comply with current law accountable by withholding Federal funds.

This legislation underscores the concept that, unbelievably, has been lost among municipalities across the country. Despite what the current administration might have us think, upholding the Federal law is not a suggestion. It is a legal requirement for all of us. We can't, in good faith, ask the American people to trust us when it comes to reforming our broken immigration system until they see us willing to stand up and enforce the laws that are currently on the books and hold those jurisdictions, municipalities, States, and other local entities that refuse to comply with Federal law accountable. That

is why organizations such as the National Sheriffs' Association and the National Association of Police Organizations have voiced their support for this legislation.

To sum up, the Stop Sanctuary Policies and Protect Americans Act really serves as a confidence-building exercise for Congress. If the American people don't see us actually stepping up and demanding that local jurisdictions enforce current law, how can they expect us to pass complex immigration reform legislation to address our broken immigration system? Unfortunately, in this confidence-building exercise, the Senate, led by our colleagues across the aisle, has failed in that confidence-building exercise. What they have done is to reinforce the belief that there are Members of the Senate who believe that local jurisdictions can openly defy Federal law and there will be no recourse and no accountability.

Frankly, it is hard for me to understand how our Democratic colleagues can, in good conscience, block this legislation, given some of the horrific crimes that have occurred, such as the crime that was committed against Kate Steinle in San Francisco. There are many, many, many tragic examples of this happening over and over in our country. This was our opportunity to do something about it, but unfortunately, for reasons unbeknownst to me, our Democratic colleagues will not even allow us to pass a bill which will hold jurisdictions that refuse to enforce current Federal law accountable.

I yield the floor.

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

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

The legislative clerk proceeded to call the roll.

Mr. THUNE. 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. THUNE. Mr. President, this week we have been discussing and taking up legislation to address the problem of sanctuary cities. In fact, just earlier today, we had a procedural vote on a motion to proceed to actually get on the bill. It failed. It only had 54 votes. The threshold in the Senate to get on a bill is 60 votes. Democrats here in the Senate decided to block consideration of this bill and to have that 60-vote threshold in play, and as a consequence, it failed. We had 54 votes. I think only two Democratic Senators voted to proceed to this legislation, and I would argue that is very unfortunate because this is a piece of legislation which represents common sense and what I think the American people want us to be focused on when it comes to the issue of dealing with crime in our communities and illegal immigration in a way that ensures that those who come to this country and commit crimes aren't allowed to stay here.

According to the Department of Homeland Security, there are 334 jurisdictions across our country right now that have official policies discouraging cooperation with Federal immigration enforcement officers. Among other things, that means these jurisdictions regularly ignore what are called detainers, requests from the Department of Homeland Security to hold an individual for deportation. As a city prepares to release an illegal immigrant who has been convicted of or charged with a crime, the Department of Homeland Security will send a detainer asking that the individual be held for a brief period—usually 48 hours—until Federal immigration officers can take custody.

In a majority of the cities across the country, law enforcement would simply comply with this request and hold the individual until the Department of Homeland Security can arrive, but in sanctuary cities officials regularly ignore these requests and simply release these individuals from jail and back into the population at large—a practice that has resulted in the release of approximately 1,000 undocumented criminals per month. According to information from U.S. Immigration and Customs Enforcement, 9,295 imprisoned individuals whom Federal officials sought to deport were released into the population between January 1 and September 30 of last year. They released 9,295 imprisoned individuals in just 9 months. Of those 9,295 individuals, 5,947, or 62 percent, had a significant prior criminal history or presented a threat to public safety even before the arrest that preceded their release, and many went on to be arrested again within a short period of time.

There is a terrible human cost to sanctuary cities' decision to refuse to cooperate with U.S. immigration law. There has been a lot of discussion on the floor about Kate Steinle. Kate Steinle paid that cost when she was murdered on a San Francisco pier while walking with her father on July 1, 2015. She was shot by an undocumented immigrant who had been convicted of no fewer than seven felonies—seven felonies—prior to the decision of the city of San Francisco to ignore a request from the Department of Homeland Security and then go on and release this man into the population.

Unfortunately, Kate Steinle is not alone. Marilyn Pharis of Santa Maria, CA, was raped and then bludgeoned by an undocumented immigrant who had previously been arrested for battery but had been released after the local sheriff's office decided to ignore a request to detain him until he could be taken into Federal custody.

A 2-year-old California girl—a 2-year-old—was brutally beaten by her mother's boyfriend, an undocumented immigrant with felony drug and drunk driving convictions, who was released on bail after the crime despite a request from Federal officials that he be detained.

In 2011, Dennis McCann was killed when he was hit and dragged by a car driven by a drunk driver with a blood alcohol content nearly four times the legal limit. His killer turned out to be Saul Chavez, an undocumented immigrant with a prior drunk driving conviction. After Dennis McCann's death, the Department of Homeland Security filed a request asking that Immigration and Customs Enforcement be notified if Chavez was scheduled to be released. Cook County, however, chose to ignore this request, and after being released on bail, Dennis's killer apparently fled the country. Four years later, Dennis's family is still waiting to see justice done.

Unfortunately, I could go on and on. Decisions to release undocumented immigrants convicted of crimes, instead of detaining them for Federal officials, have resulted in far too many tragedies like those of Marilyn Pharis and Kate Steinle, and too many families in this country are mourning as a result.

Cooperation between local and Federal law enforcement is essential to protecting Americans, and detainer requests from the Department of Homeland Security are a key tool that helps Federal officials make sure dangerous individuals are not going back onto our Nation's streets.

When cities and counties ignore these requests, they force immigration officers to attempt to track down undocumented criminals after they have been released into the community. According to the Center for Immigration Studies, this requires an exponentially larger expenditure of funds and manpower and success is not guaranteed. Immigration and Customs Enforcement needs the support of cities and local law enforcement if it is going to keep these individuals off our Nation's streets.

The legislation we have been discussing today would take a substantial step forward toward handling the threat posed by sanctuary cities. The Stop Sanctuary Policies and Protect Americans Act, which has strong support from law enforcement organizations and victims' families, will withhold Federal funds under three grant programs and redirect those funds to jurisdictions that comply with Federal immigration laws. It will also provide crucial legal protections to law enforcement officers that will allow them to cooperate with Federal immigration authorities without the fear of lawsuits.

This act also incorporates provisions known as Kate's Law, named after Kate Steinle. These provisions would increase the maximum penalty for illegally reentering the United States after being deported and create a maximum penalty of 10 years for reentering the country illegally after being deported three or more times. Kate's Law would also create a mandatory minimum sentence of 5 years for those reentering the country after having been convicted of an aggravated felony prior to deportation or for those who reenter the country after two previous convictions for illegal reentry.

What happened to Kate Steinle on that pier in San Francisco should never have happened. It likely could have been prevented if San Francisco had chosen to respect the Department of Homeland Security's request to hold her killer until immigration officers could pick him up.

I hope the stop sanctuary policies act will move forward in the Senate so we will be able to send a version of this legislation to the President. It is time we started ensuring that dangerous criminals like Kate Steinle's killer don't end up back on the streets. We have that opportunity today. We ought to vote to move to this bill.

What is truly remarkable and amazing is that we couldn't even get on the bill to debate it. It was blocked by our colleagues on the other side who prevented even proceeding to the bill—a motion to proceed, which takes 60 votes in the Senate. It would have been very easy to get on the bill and at least have that debate. If they didn't like the provisions in the bill, they would have an opportunity to amend it and discuss the bill as we should be doing in the Senate, but instead the Democratic Senators chose to block the consideration, even the very consideration of legislation that would go to great lengths to try and prevent the types of tragedies we witnessed this last summer with Kate Steinle and so many others who have fallen prey to acts of violence by those who are here illegally and have prior experience with the law, prior convictions, and who are clear dangers to people and families all across this country.

It is a tragedy we weren't able to get on the bill. I hope our Democratic colleagues will change their minds and allow us to proceed to this legislation, to debate it, to vote on it, to pass it, and to send it to the President for his signature.

CYBERSECURITY INFORMATION SHARING BILL

Mr. President, I also wish to speak in support of S. 754, which I think we will be discussing momentarily, the Cybersecurity Information Sharing Act, or what is referred to as CISA, which the Senate is going to be debating this week. I commend Chairman BURR and Vice Chairman FEINSTEIN for their bipartisan work to bring this bill to the floor.

It seems that every week we learn of another serious cyber attack against U.S. businesses and government agencies. The most devastating recent attack is the one against the Office of Personnel Management that compromised the background check information of more than 21 million Americans. The pace of such attacks appears to be accelerating. According to the security firm Symantec, last year alone, more than 300 million new types of malicious software or computer viruses were introduced on the Web or nearly, if my colleagues can believe this, 1 million new threats each and every day.

Just last month, Director of National Intelligence James Clapper testified before the House Intelligence Committee that ''cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact.''

From my position as head of the Senate commerce committee, I have promoted the great potential of the emerging Internet of Things—which promises to yield improvements in convenience, efficiency, and safety by connecting everyday products to the Web—but I have also held several hearings on the cyber security risks and challenges that accompany an increasingly connected world. By increasing the sharing of cyber threat information between and among the private and public sectors, the bill would authorize the voluntary sharing of cyber threat information and would provide commonsense liability protections for companies that share such information with the government or their peers, when they abide by the bill's requirements. The goal is to help companies and the government better protect their networks from malicious cyber attacks by sharing information about those threats earlier and more broadly.

Similar bipartisan legislation was reported by the Senate Intelligence Committee last year that was never considered by the Democratic-controlled Senate at the time. This year the Intelligence Committee passed a bill by a bipartisan vote of 14 to 1, which should portend a strong bipartisan vote on the floor of the Senate.

The House of Representatives has also passed two bills to facilitate the sharing of cyber threats, so we are now within striking distance of finally enacting critical cyber security information-sharing legislation after several false starts in recent years.

I know some have questioned whether this bill provides appropriate protections for personal privacy and civil liberties. I appreciate these concerns, and I believe the bill's sponsors have meaningfully addressed them, including through modifications to be included in a managers' amendment.

This bill is not a surveillance bill. Among other things, the modified bill would limit the sharing of information to that defined as ''cyber threat indicators'' and ''defensive measures'' taken to detect, prevent or mitigate cyber security threats.

The bill also requires private sector and Federal entities to remove personally identifiable information prior to sharing threat indicators, and the Federal Government can only use the cyber threat information it receives for cyber security purposes and to address a narrow set of crimes, such as the sexual exploitation of children.

The bill also requires regular oversight of the government's sharing activities by the Privacy and Civil Liberties Oversight Board created after 9/11 and by relevant agency inspectors general.

In the end, it is important to remember that CISA is about cyber threats—like the malware being used by criminals in hostile states—not personal information. Meanwhile, failing to enact this bill could actually make it easier for criminals in rogue states to continue collecting our personal information from vulnerable systems.

Let me be clear. This is not a silver bullet and it will not render cyberspace completely safe—no bill can do that—but CISA is an important piece of the ongoing effort to improve our cyber security.

Late last year, after a decade without passing major cyber security legislation, Congress enacted five cyber security laws that target other pieces of the cyber puzzle. I coauthored one of these—the Cybersecurity Enhancement Act—with former Senator Jay Rockefeller. This law ensures the continuation of a voluntary and private sector-led process at the Commerce Department's National Institute of Standards and Technology, or what we refer to as NIST, to identify best practices to protect our Nation's critical infrastructure from cyber threats. The Cybersecurity Enhancement Act also promotes cutting-edge research, public awareness of cyber security risks, and improvements in our cyber security workforce.

CISA will work together with this new law and others to ensure that businesses have timely warning about current threats so they can better protect themselves—and all of us—from cyber attacks. It does so in a manner that protects individual privacy and avoids government mandates.

I look forward to the coming debate on the bill—including a healthy consideration of amendments—and I urge my colleagues to join the bipartisan sponsors and a broad coalition of stakeholders around this country in supporting this much needed legislation.

I yield the floor.

The PRESIDING OFFICER. The Senator from Oregon.

Mr. WYDEN. Mr. President, since we are still on the sanctuaries bill, before we turn to the cyber legislation, I ask unanimous consent that I be allowed to address the Senate after Chairman BURR has completed his remarks and after Ranking Member FEINSTEIN has completed her remarks.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Mr. President, we are quickly moving to a point where I think the majority leader will come to the floor and will call up the cyber security bill.

Let me remind my colleagues that we have been on the floor briefly before, and the conclusion then was that we agreed to a unanimous consent request that made in order 22 amendments. It was not a limiting UC. So there is the opportunity for additional amendments to come to the floor.

As we start, I say to my colleagues that if we have a level of cooperation

by the Members—if in fact they come, debate, and vote on amendments—we can resolve this in literally a matter of a couple of days. If people want to try to obstruct, then it is going to be a lengthy process procedurally.

I don't think there is a lot new that we are going to learn. What is the fact? The fact is that actors around the world continue to attack U.S. systems and, in many cases, penetrate them: Sony Films, Anthem Health, OPM.

The Presiding Officer, as a member of our committee, knows that the amount of personal data that is being accumulated out there somewhere provides almost a roadmap to everything about anybody. What we are attempting to do with this cyber bill I want the American people to understand: This is not to prevent cyber attacks. I would love to figure out technologically how we do it. Nobody has been able to do it. What this is designed to do is to minimize the data that is lost, to minimize the personal information that an individual gleans out of going into a database and pulling out that information.

The vice chairman and I have worked with other members of the committee to report a bill out of the committee on a 14-to-1 vote. We are now almost 3 months behind the House of Representatives, which has passed two bills that we desperately need to get out of the Senate in a piece of legislation that we could conference with the House of Representatives. In a conversation just this morning that I had with the White House, they are supportive of this bill getting out of the Senate and having the bill on the President's desk so that he could sign it into law and we could have this in place.

Let me make some overall points on the cyber bill. One, most importantly, it is voluntary. Any business in America can choose to participate or not to participate. They can tell the Federal Government that they have been penetrated. They can provide the appropriate data for us to begin the forensics and to tell them in real time: Here is a defensive software package you can put on your system that will make it immune from that tool again. But more importantly, it might minimize the amount of data that is lost and certainly would allow the government to then broadcast to business more widely: Here is the tool that is being used today and here is the defensive mechanism to keep other businesses from having the same penetration and data loss.

Now, it is important that I say that when we started there were 22 amendments that were placed in order. I am proud to tell my colleagues that we have worked out eight of those amendments. They will be incorporated in a managers' amendment that will also have an additional six amendments that we think strengthen the concerns that have been expressed about privacy. They also address certain areas of cross-jurisdiction, such as the Department of Homeland Security. We now have those chairmen and those ranking members fully on board in support of this legislation. Now we have to go through the process. At the root of this is moving forward a piece of legislation on cyber that is a voluntary piece of legislation by companies.

I mentioned real time. I know the Presiding Officer has heard this in committee. If we can't promise real time, we can't promise to anybody who is willing to provide the data that we can actually stop or minimize data loss. So it is absolutely crucial that this all function in real time. To have a voluntary program that involves real time transfer of information means that there have to be incentives for that to be done.

Let me just point out two things. For a company to talk to a competitor after they have been attacked and penetrated, we provide antitrust protection to them to talk directly to that competitor as fast as they possibly can to find out whether we have multiple systems that are at risk. For the company to report to the Federal Government we provide liability protection just for the transfer of that information. As Members read the bill, they will see that statutorily we don't allow personal data that is unrelated to the forensics—needed to identify who did the attack, with what type of a tool, and what the defensive mechanism is—that statutorily cannot be transferred from a private company to the government. Additionally, we say to every Federal agency that might receive in real time this data that if there is personal data that is transmitted from a company to the Federal Government, you cannot distribute personal data.

I am not sure how it gets stronger than where we are, but I have come to this conclusion after working on this legislation for this entire year—and the vice chairman has worked on it for multiple years: There are some people who don't want legislation. We have met with every person who had a good thought—legislation that would send us in a positive direction but still embrace the policy found in this legislation. It is limited, but there are some who we can't in fact satisfy.

So let me say this to those companies that have expressed opposition to this piece of legislation. It is really clear. Choose not to participate. It is voluntary. To those companies that find no value in it, if you have an aversion to what we have written, don't participate—even though a majority of businesses in America are actually calling my office and the vice chairman's office saying: When are we going to get this done? We need this. We need it.

It is that simple. That is the beauty of it being voluntary. Voluntary also means that the U.S. Chamber of Commerce is 100 percent supportive of this legislation. Now we never have full agreement from a membership of an association, but it takes a majority—in fact, it takes well over a majority—for an organization such as that to come out publicly supporting it. So I say very boldly, if you don't like the piece of legislation, it is real easy: You just don't participate in it.

Some have called this a surveillance bill. Let me just knock that down real quick. First, this bill requires private companies and the government to eliminate any irrelevant personal, identifiable information before sharing cyber threat indicators or defensive measures. Second, this bill does not allow the government to monitor private networks or computers. Third, this bill does not allow the government to shut down Web sites or require companies to turn over personal information. Fourth, this bill does not permit the government to retain or use cyber threat information for anything other than cyber security purposes, identifying the cyber security threat, protecting individuals from death or serious bodily or economic harm, and protecting minors or investigating limited cyber crime offenses. Fifth, it provides rigorous oversight and requires a periodic interagency inspector general report to assess whether the government has violated any of the requirements found in this act. The report would also assess any impact this bill may have on privacy and civil liberties.

Finally, our managers' amendment has incorporated additional provisions that enhance privacy protection. First, our managers' amendment omitted the government's ability to use cyber information to investigate or prosecute serious violent felonies.

Personally, I thought that was a pretty good thing. I can understand where it is outside of the scope of a cyber bill, but information about a felony that you learned in this I thought was something the American people would want us to act on. Individuals raised issues on it. We dropped it out of the bill.

Secondly, our managers' amendment limited cyber threat information sharing authorities to those that are shared for cyber security purposes. In other words, it is only for cyber security purposes.

Both of these changes ensure that nothing in our bill reaches beyond the focused cyber security threats that it intends to prevent and deter. Nothing in this bill creates any potential for surveillance authorities. Despite rumors to the contrary, CISA's voluntary cyber threat indicator sharing authorities do not provide in any way for the government to spy on or use library and book records, gun sales, tax records, educational records or medical records. Given that cyber hackers have hacked into and stolen so much publicly disclosed private, personal information, it is astounding that privacy groups would oppose a bill that has nothing to do with surveillance and seeks to protect their private information from being stolen. I guess that has been the most troubling aspect of the road we have traveled—that we are trying to protect personal data, and yet

the groups that say they are the stewards of personal data are the ones that, in fact, are the most vocal on this.

CISA ensures the government cannot install, employ or otherwise use cyber security systems on private sector networks. No one can hack back into a company computer system even if their purpose is to protest against or quash cyber attacks.

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

That is what we are here talking about. This is voluntary and it is targeted at minimizing data loss. It is targeted at trying to protect the personal data of the American people found in every database in every company around the world.

Mr. President, I am going to turn to my vice chairman as we get ready for Senator WYDEN to make remarks and for leader MCCONNELL to come to the floor.

I would put Members on notice once again. It is our intent to have some opening comments, to actually make the managers' amendment pending, to make those amendments that were part of the unanimous consent agreement but not worked out as part of the managers' package pending.

I encourage those Members who have authorship of those pending amendments to come and debate them, and we will schedule a vote for them. If you have additional amendments, come and offer those amendments and we will start debate on it. It is our goal, with the cooperation of Members, to work expeditiously through all of the amendments one wants to consider and to dispose of them and to finalize cyber security legislation in the Senate so we can move to the House and conference a bill.

I yield the floor.

The PRESIDING OFFICER. The Senator from California.

Mrs. FEINSTEIN. Mr. President, I want to begin by saying that I very much agree with what Chairman BURR has just stated. It is factual. It is the truth.

For me, I have worked on this issue for 7 years now. And this is actually the third bill that we have tried to move.

I want to thank the two leaders for bringing the bill to the floor, and I hope it can be considered quickly.

Up front I want to make clear, if it hasn't been made clear, that this legislation is a first step only to improve our Nation's defenses against cyber attack and cyber intrusion. It is not a panacea, and it will not end our vulnerabilities. But it is the most effective first legislative step we believe that we can take.

This legislation is about providing legal clarity and legal protection so that companies can share cyber threat information voluntarily with each other and with the government. It provides companies the protections they need and puts strong privacy rules in place.

At the beginning of this debate, I think it is important to talk about the depth and breadth of the cyber threat we actually face every day, because rarely does a month go by without the announcement of a significant cyber attack or intrusion on an American company or an agency of the U.S. Government. These attacks compromise sensitive personal information, intellectual property or both.

Just in the last year, major banks, health insurers, tech companies, and retailers have seen tens of millions of their customers' sensitive data stolen through cyber means. In 2014 the Internet security company Symantec reported that over 348 million identities were exposed through data breaches. Threats in cyber space do not just risk the personal data of Americans. They are a significant and growing drain on our economy as malicious actors steal our money, rob companies of intellectual property, and threaten our ability to innovate.

The cyber security company McAfee and the think tank Center for Strategic and International Studies estimated last year that the cost of cyber crime is more than $400 billion annually. The same study stated that losses from cyber theft could cost the United States as many as 200,000 jobs. These are not theoretical risks; they are happening today and every day.

As we know all too well in the wake of cyber intrusions at the Office of Personnel Management, cyber threats are not only aimed against the private sector. They are also aimed against the public sector. Every day, foreign nation-states and cyber criminals scour U.S. Government systems and our defense industrial base for information on government programs and personnel—every single day.

More than 22 million government employees and security clearance applicants had massive amounts of personal information stolen from the Office of Personnel Management, reportedly taken by China. These employees now face increased risk of theft and fraud, and also their information could be used for intelligence operations against them and the United States.

As bad as this is—and it is bad—we have seen in the last few years an acceleration of an even more concerning trend, that of cyber attack instead of just cyber theft. In 2012 major U.S. financial institutions saw an unprecedented wave of denial-of-service attacks on their systems.

Saudi Aramco—reported to be the world's largest oil and gas company—was the victim of a cyber attack that wiped out a reported three-quarters of its corporate computers. In 2013 we saw further escalations of these threats as waves of denial-of-service attacks were aimed at some of our largest banks. In early 2014 Iran launched a cyber attack on the Sands Casino which, according to the public testimony of the Director of National Intelligence, James Clapper, rendered thousands of computer systems inoperable. Last November we saw one of the most publicized cyber attacks when North Korean attacks broke into Sony Pictures Entertainment, stole vast amounts of sensitive and personal data, and destroyed the company's internal network.

These breaches of personal information and loss of intellectual property and destructive attacks continue online every day. It is only a matter of time before America's critical infrastructure—major banks, the electric grid, dams, waterways, the air traffic control system, and others—is targeted for a cyber attack that could seriously affect hundreds of thousands of lives.

Clearly it is well beyond the time to act. There is no legislative or administrative step we can take that will end cyber crimes and cyber warfare. However, since the Intelligence Committee began looking seriously at this in 2008, we have heard consistently that improving the exchange of information about cyber threats and cyber vulnerabilities can yield a real and significant improvement to U.S. cyber security. That is why this bill is the top cyber legislative priority for the Congress, the Obama administration, and the business community.

I have heard directly from dozens of corporate executives about the importance of cyber security legislation, as have the Intelligence Committee staff in hundreds of meetings over the course of years in drafting this legislation. As Chairman BURR has said, not only has the U.S. Chamber of Commerce called for this legislation but so have dozens—specifically 52—of industry groups representing some of the largest sectors of our economy. On the floor in early August, I listed 40 associations that have written in support of the legislation. Today there are 52.

I ask unanimous consent that the list of supporters of this bill be printed in the RECORD.

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

CYBERSECURITY INFORMATION SHARING ACT

ENDORSEMENTS

Agricultural Retailers Association, Airlines for America, Alliance of Automobile Manufacturers, American Bankers Association, American Cable Association, American Chemistry Council, American Coatings Association, American Fuel & Petrochemical Manufacturers, American Gaming Association, American Gas Association, American Insurance Association American Petroleum Institute.

American Public Power Association, American Water Works Association, ASIS International, Association of American Railroads, Association of Metropolitan Water Agencies, BITS—Financial Services Roundtable, College of Healthcare Information Management,

Computing Technology Industry Association, Executives Computing Technology Industry Association, Edison Electric Institute, Electronic Payments Coalition, Electronic Transactions Association, Federation of American Hospitals, Food Marketing Institute.

Global Automakers, GridWise Alliance, Healthcare Information and Management Systems Society, Health Information Trust Alliance, Large Public Power Council, National Association of Chemical Distributors, National Association of Manufacturers, National Association of Mutual Insurance Companies, National Association of Water Companies, National Business Coalition on e-Commerce & Privacy, National Cable & Telecommunications Association, National Retail Federation.

National Rural Electric Cooperative Association, Property Casualty Insurers Association of America, Real Estate Roundtable, Retail Industry Leaders Association, Rural Broadband Association, Security Industry Association, Software & Information Industry Association, Society of Chemical Manufacturers & Affiliates, Telecommunications Industry Association, Transmission Access Policy Study Group, United States Telecom Association, U.S. Chamber of Commerce, Utilities Telecom Council, Wireless Association.

Mrs. FEINSTEIN. Mr. President, regrettably this is the third attempt to pass a cyber security information sharing bill in recent years. In 2012 the Lieberman-Collins Cybersecurity Act of 2012 was on the floor. It included a title on information sharing which the Intelligence Committee helped produce. It was an important piece of legislation, but it only received one Republican vote.

Last Congress, then-vice chairman of the Intelligence Committee Saxby Chambliss and I set out to draft a narrower bill just on information sharing in the hopes of attracting bipartisan support. The Intelligence Committee approved a bill in 2014 by a strong bipartisan vote of 12 to 3, but it never reached the Senate floor due to privacy concerns. So this is the third try.

I am very pleased that Chairman BURR and I now have the opportunity to bring a bill to the floor that both sides can and should support. This bill is bipartisan. It is narrowly focused. It puts in place a number of privacy protections, many of which we will outline shortly. I believe the bipartisan vote of 14 to 1 in the Senate Intelligence Committee in March underscores this fact. I would like to commend Senator BURR's leadership and his willingness to negotiate a bipartisan bill with me that can and should—and I hope will—receive a strong vote in the Senate. Let me take a few minutes to describe the main features of the bill and its privacy protections.

In short, it does the following five things:

First, the bill recognizes that the Federal Government has information about cyber threats that it can and should share with the private sector and with State, local, and tribal governments. The bill requires the Director of National Intelligence to put in place a process to increase the sharing of information on cyber threats already in the government's hands with the private sector to help protect an individual or a business. So that is the sharing between the government and the private sector. This includes sharing classified data with those with security clearances and an appropriate need to know but also requires the DNI to set up a process to declassify more information to help all companies secure their networks. We have heard over and over again from companies that the information they get from the government today is not sufficient. That needs to change.

Second, the bill provides clear authorization for private sector entities to take appropriate actions. That includes an authorization for a company to monitor its networks or information on its networks for cyber security purposes only. No other type of monitoring is permitted, nor is the use of information acquired through such monitoring allowed for purposes other than cyber security.

There is also an authorization for a company to implement a defensive measure on its network to detect, prevent, or mitigate a cyber threat. This authorization by definition does not authorize a defensive measure that destroys, renders unusable, or substantially harms a computer system or information on someone else's network. This is an important point. There has been concern that the bill would immunize a company for damage it might cause to other people's networks. The managers' amendment makes clear that the authorization in this bill allows companies to block malicious traffic coming from outside their network and stop threats on their systems but not conduct offensive activities or otherwise have substantial effects off their networks.

Finally, there is an authorization for companies to share limited cyber threat information or defensive measures with other companies or with government agencies. It does not authorize sharing anything other than cyber information. In a critical change, the managers' amendment states that sharing is for cyber security purposes only. So this really is a very limited authorization.

It is important to note that while these activities are authorized, they are not mandatory. Information sharing, monitoring, and use of defensive measures are all voluntary. The bill makes explicit that there are no requirements for a company to act or not to act.

I have heard from technology companies in the past couple of weeks that they are concerned that this bill requires them to share customer information with the government. That is false. Companies can choose to participate or they can choose not to. If they do, they can only share cyber threat information, not their company's personal information or their online activity.

The third thing this bill does is it puts in place procedures and limitations for how the government will receive, handle, and use cyber information provided by the private sector. The bill requires two sets of policies and procedures. The first set—to be written by the Attorney General and the Secretary of Homeland Security—requires that cyber information that comes to the Federal Government will be made available to all appropriate Federal departments and agencies without unnecessary delay and that the information sharing system inside the government is auditable and is consistent with privacy safeguards.

The second set of required guidelines is designed to limit the privacy impact of the sharing of cyber information and specifically limits the government's receipt, retention, use, and dissemination of personal information. These guidelines are to be written by the Attorney General. They will be made public.

The bill specifically limits the use of cyber information by the government. Federal agencies can only use the information received through this bill for a cyber security purpose, for the purpose of identifying a cyber threat, preventing or responding to an imminent threat of death, serious bodily harm, serious economic harm, including an imminent terrorist attack, preventing or responding to a serious threat of harm to a minor, and preventing, investigating, or prosecuting specific cyber-related crimes.

Fourth, the bill creates what we call in shorthand a portal at the Department of Homeland Security and requires that cyber information is received by the government through the Homeland Security portal, from which it can be distributed quickly and responsibly to appropriate departments and agencies. This portal was the joint proposal a few years ago by former DHS Secretary Janet Napolitano, FBI Director Bob Mueller, and NSA Director Keith Alexander. The purpose of the portal is to centralize the entry point for cyber information sharing so that the government can effectively and efficiently receive that cyber information, can protect privacy, and can ensure that all the appropriate departments with cyber security responsibility can quickly learn about threats.

A key aspect of this centralized portal is to enable information to move where it needs to go automatically. Once cyber threat information enters the portal, it will be shared in real time—meaning without human intervention and at machine speed—to the other appropriate Federal agencies. The belief is that they can put in a filter and do a privacy scrub, if you will, just in case there is any private information, such as a Social Security number, a driver's license number, or something like that, that can be instantly moved out.

Such a real-time exchange is necessary because if there are indications that a cyber attack is underway, the

response to stop that attack will need to be immediate and not subject to any delay. The bill makes clear that this can and should be done in a way that ensures that privacy is protected, improving both privacy protections and the ability to quickly protect sensitive systems.

Fifth and finally, the bill provides liability protection to companies that act in accord with the bill's provisions. Specifically, the bill provides liability protection for companies that properly monitor their computer networks or that share information the way the bill allows. The bill specifically does not protect companies from liability in the case of gross negligence or willful misconduct, nor does it protect those who do not follow its privacy protections.

As I mentioned earlier, there are many privacy protections throughout the bill. Because this is a key point of interest for a number of Senators, I wish to list 10 of them.

No. 1, it is voluntary. The bill doesn't require companies to do anything they choose not to do. There is no requirement to share information with another company or with the government, and the government cannot compel any sharing by the private sector. So if there is this tech company or that tech company that doesn't want to provide this information, don't do it. Nothing forces you to do it. This is 100 percent voluntary.

No. 2, it narrowly defines the term ''cyber threat indicator'' to limit the amount of information that may be shared under the bill. Only information that is necessary to describe or identify cyber threats can be shared.

No. 3, the authorizations are clear, but they are limited. Companies are fully authorized to do three things: monitor their networks or provide monitoring services to their customers to identify cyber threats, use limited defensive measures to protect against cyber threats on their networks, and share and receive cyber information with each other and with Federal, State or local governments. No surveillance, no sharing of personal or customer information is allowed.

No. 4, there are mandatory steps that companies must take before sharing any cyber threat information with other companies or the government. Companies must review information before it is shared for irrelevant privacy information, and they are required to remove any such information that is found. A bank would not be able to share a customer's name or account information. Social Security numbers, addresses, passwords, and credit information would be unrelated to a cyber threat and would, except in very exceptional circumstances, be removed by the company before sharing.

No. 5, the bill requires that the Attorney General establish mandatory guidelines to protect the privacy of any information the government receives. These guidelines will be public. The guidelines will limit how long the government can retain any information and provide notification requirements and a process to destroy mistakenly shared information. It also requires the Attorney General to create sanctions for any government official who does not follow these mandatory privacy guidelines.

No. 6, the Department of Homeland Security, not the Department of Defense or the intelligence community, is the primary recipient of the shared cyber information.

No. 7, the managers' amendment includes a new provision, which was suggested by Senator CARPER, with the backing of a number of privacy groups, to allow the Department of Homeland Security—and I say this again—to scrub the data as it goes through the portal to make sure it does not contain irrelevant personal information.

No. 8, the bill restricts the government's use of voluntarily shared information to cyber security efforts, imminent threats to public safety, protection of minors, and cyber crimes. Unlike previous versions, the government cannot use this information for general counterterrorism analysis or to prosecute noncyber crimes.

No. 9, the bill limits liability protection to only monitoring for cyber threats and sharing information about them when a company complies with the bill's privacy requirements, and it explicitly excludes protection for gross negligence or willful misconduct.

No. 10, above and beyond these mandatory protections, there are a number of oversight mechanisms in the bill which involve Congress, the heads of agencies, the inspectors general, and the Privacy and Civil Liberties Oversight Board.

In sum, this bill allows for strictly voluntary sharing of cyber security information with many layers of privacy protections.

As I have noted, the managers' amendment that we will consider shortly, I hope, will include several key privacy protections. We will be describing them in more detail when we turn to that amendment.

Mr. President, I hope this has made clear that we have tried to very carefully balance the need for improved cyber security with the need to protect privacy and private sector interests. As I said earlier, this is the third bill on information sharing. We have learned from the prior two efforts.

It is clear from the headlines and multiple data breach notifications that customers and employees are now receiving that this bill is necessary and we need to act now instead of after a major cyber attack seriously impacts hundreds or thousands of lives or costs us billions or trillions of dollars.

We have a good bill. I know there are some cynics. I know there are some tech companies that may be worried about what their customers might do. Then don't participate if you don't want to, but I have talked to enough CEOs who have said to me: Please do this. We need this ability to share, and the only way we can get this ability is with liability protection for sharing cyber threat material, so this is very important.

I again thank the chairman for everything he has done to lead this effort. It is my hope that we will have a good, civil debate and that we will be able to pass this bill with a substantial margin.

I yield the floor.

The PRESIDING OFFICER. The Senator from Oregon.

Mr. WYDEN. Mr. President, this afternoon we begin the discussion of cyber security legislation. I think it is important to say at the outset that I think everybody who hears the notion that the Senate is talking about cyber security would say: Boy, you have to be for that. We all read about cyber hacks regularly, so you ask: Why not be for what they are talking about in the Senate?

I begin by way of saying that the fact is not every bill with cyber security in the title is necessarily a good idea. I believe this bill will do little to make Americans safer but will potentially reduce the personal privacy of millions of Americans in a very substantial way. In the beginning, I think it is particularly telling who opposes this legislation at this time. The Business Software Alliance has said they cannot support this bill. They have members such as Apple, IBM, and Microsoft, and they are saying that at this time they cannot be for this bill. The Computer and Communications Industry Association has members such as Google, Facebook, and Amazon. They have said they cannot support the legislation at this time. America's librarians cannot support it at this time. Twitter cannot support it at this time. Wikimedia Foundation and Yelp can't support it at this time.

The groups I am talking about are ones with members who have companies with millions and millions of customers, and they are saying they can't support this bill at this time.

I think I know why these companies that didn't have a problem with previous kinds of versions of this legislation are saying they don't support it. These companies are hearing from their customers and they are worried their customers are saying: This doesn't look like it is going to protect our privacy. Of course, we want to be safe. We also want to have our liberty. Ben Franklin famously said anyone who gives up their liberty to have security really doesn't deserve either—so we know what Americans want.

I would submit the reason these companies are coming out in opposition to this legislation is they don't want their customers to lose confidence in their products. They are looking at this legislation, and they are saying the privacy protections are woefully inadequate and their customers are going to lose confidence in their products.

I appreciate that the managers are trying to make the bill better. It is

quite clear to me, having listened to two colleagues—whom I respect very much—that they are very much aware that their bill has attracted widespread opposition. The comment was made that Apple, Google, everyone should be for this.

I would say again—respectfully to my colleagues, the authors, with whom I have served since we all came to the committee together—even with the managers' amendment, the core privacy issues are not being dealt with.

I would just read now from a few of the comments—maybe I am missing something. Maybe I heard a list of all the privacy issues that had been addressed. I haven't seen any privacy groups the Democrats or Republicans look to saying they support the privacy protections in the bill, but let me give you an example of a few who surely don't.

This is what Yelp says: ''Congress is trying to pass a 'cyber security' bill that threatens your privacy.''

This is what the American Library Association is saying. I will admit, Mr. President, I am a little bit tilted toward librarians because my late mother was a librarian. We all appreciate the librarians we grew up with. The librarians say that this bill ''de facto grants broad new mass data collection powers to many federal, as well as state and even local government agencies.''

Salesforce, a major player in the digital space located in California, says:

At Salesforce, trust is our number one value and nothing is more important to our company than the privacy of our customers' data. . . . Salesforce does not support CISA and has never supported CISA.

They have a hashtag.

Follow #StopCISA for updates.

This is the group that represents the Computer and Communications Industry Association—this is Google, Amazon, and Microsoft, the biggest major tech companies. Again, these are companies with millions of customers, and the companies are worried that this bill lacks privacy protections and their customers are going to lose confidence in some of what may be done under this. They say they support the goals, of course—which we all do—of dealing with real threats and sharing information. They state: ''But such a system should not come at the expense of users' privacy, need not be used for purposes unrelated to cyber security, and must not enable activities that might actively destabilize the infrastructure the bill aims to protect.''

Mr. President, we heard my colleague, the chair of the committee, a member of the Committee on Finance whom I have worked with often, say that the most important feature of the legislation is that it is voluntary. The fact is that it is voluntary for companies. It will be mandatory for their customers. And the fact is that companies can participate without the knowledge and consent of their customers, and they are immune from customer oversight and lawsuits if they do so. I am all for companies sharing information about malware and foreign hackers with the government, but there ought to be a strong requirement to filter out unrelated personal information about customers.

I want to emphasize this because this is probably my strongest point of disagreement with my friends who are the sponsors. There is not in this bill a strong requirement to filter out unrelated personal information about these millions of customers who are going to be affected. This bill would allow companies to hand over a large amount of private and personal information about millions of their customers with only a cursory review. In my judgment, information about those who have been victims of hacks should not be treated in essentially the same way as information about the hackers. Without a strong requirement to filter out unrelated personal information, that is unfortunately what this bill does.

At the outset of this discussion, we were told this bill would have substantial security benefits. I heard for days, for example, that this bill would have prevented the OPM attack, that it would have stopped the serious attack on government personnel records. After technologists reviewed that particular argument, that claim has essentially been withdrawn.

There is a saying now in the cyber security field: If you can't protect it, don't collect it. If more personal consumer information flows to the government without strong protections, my view is it is going to end up being a prime target for hackers.

Sharing information about cyber security threats is clearly a worthy goal, and I would like to find ways to encourage more of that responsibly. Yet if you share more information without strong privacy protections, millions of Americans will say: That is not a cyber security bill; it is a surveillance bill. My hope is that, working in a bipartisan way, by the time we have completed this legislation on the floor, that will not be the case.

Mr. President, I yield the floor.

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, I listened patiently to my friend and colleague, and we are on the committee together, so this is not the first time we have had a frank discussion. But let me say to those companies that have reached out to him, and he listed them—I am not going to bother going through 53 associations and the number of companies that are represented because there are hundreds and hundreds. They are sectors of our economy. It is the financial industry. It is automotive. It is practically everybody in retail.

There are a couple of things that still shock me because I really can't make the connection. A technology company has a tremendous amount of users, and those users put their personal data on that—pick one—and the company says there is nothing more important than protecting the data of their users. It strikes me, because I was in business for 17 years before I came to this insane place, that any business in the world would say: I don't have a problem with putting this in place as long as I don't have to use it. I can make a decision whether I use it or whether I don't.

It may be that when they get an opportunity to see the final product and it is in place, they may say: Well, you know what, this isn't so bad. This actually took care of some of the concerns we have.

But to make a blanket statement for a company whose No. 1 concern is the protection of its customers' data—to ignore the threat today that is real and will be felt by everybody, if it hasn't been felt by them, and not have something in place is irresponsible by those companies.

Again, I point to the fact that if this were a mandatory program, I could understand why they might, for market share reasons or marketing reasons, go out and say: We are not covered by this. But this is voluntary for everybody. There is not a soul in the world who has to participate. But the ones that are really concerned about their customers' data, the ones that really understand there are companies, individuals, and countries trying to hack their systems will succumb to the fact that something is better than nothing.

It is sort of like going home to North Carolina—and I see the leader is coming—where this year we have had a rash of sharks. It is one thing to know there are sharks out there and swim and say: How could one bite me? Well, you know you have hackers out there. It seems as if you take precautions when you go swimming, and it seems as if you should take precautions to keep from being hacked.

With that, I yield the floor.

The PRESIDING OFFICER. The majority leader.

CYBERSECURITY INFORMATION SHARING ACT of 2015

Mr. MCCONNELL. Mr. President, under the order of August 5, 2015, I ask that the Chair lay before the Senate S. 754.

The PRESIDING OFFICER. Under the previous order, the Senate will proceed to the 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.