United States of America

Congressional Record

PROCEEDINGS AND DEBATES OF THE 114th CONGRESS, FIRST SESSION

Vol. 161 WASHINGTON, TUESDAY, OCTOBER 20, 2015 No. 153

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.

Righteous and Holy God, we worship You. We see Your glory in the beauty of sunrise and the splendor of sunset. Great and marvelous are Your works, for Your faithfulness sustains us. Guide our lawmakers to connect to Your eternal, essential, and unchanging holiness. With the power of Your righteous presence, renew their minds, cleanse their hearts, and guide their steps. Liberate them from the chains of pessimism, reminding them that all things are possible to those who believe. Lord, thank You for the wonder of Your love, the beauty of Your mercy, and the power of Your grace.

We pray in Your Holy 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.

SANCTUARY CITIES BILL

Mr. MCCONNELL. Mr. President, just before the State work period, I asked Senators to consider some important questions: In a time of limited Federal resources and tough choices, is it fair to treat localities that cooperate with Federal law enforcement or work hard to follow Federal law no better than localities that refuse to help or actually actively flout the law? When a deputy sheriff puts her life on the line every day, is it fair to make her live in constant fear of being sued for simply trying to keep us safe? When felons enter our country illegally and repeatedly, is it fair to victims and families to not do what we can now to stop them?

The answer is that it isn't fair. That is why colleagues should support the legislation we will consider this afternoon. It aims to ensure more fairness to cities and States that do the right thing, redirecting certain Federal funds to them from those that choose not to do the right thing. It aims to support law enforcement officers who risk everything for our safety, protecting them from lawsuits for simply doing their federally mandated duties. It aims to deliver justice for victims and their families, substantially increasing deterrence for criminals who commit felonies and then try to illegally reenter our country—endeavoring to save more Americans from the pain these families continue to experience every day.

We all know the heartbreaking story of Kate Steinle. Kate was walking arm in arm with her father one moment, begging for help the next as she began bleeding to death in his arms. The man who ended her life shouldn't have even been there that day. He had been convicted of seven—seven—felonies and deported five times, but San Francisco is a so-called sanctuary city that arbitrarily decides when it will cooperate with the Federal Government and when it will not, and it refused to even honor the Federal Government's request for an immigration detainer.

What happened to Kate is tragic, and it is not an isolated incident. Consider this letter from Susan Oliver, who lost her husband just last year. Here is what she had to say:

The man that killed my husband, Deputy Danny Oliver, was deported several times for various felonies. However, due to the lack of coordination between law enforcement agencies, his killer was allowed back into the country. . . .

I [am] asking for only one thing. I do not want your sympathy, I want change so others will not have to endure the grief we have in our lives every day.

The bill which we will consider this afternoon is supported by law enforcement organizations such as the National Sheriffs' Association, the Federal Law Enforcement Officers Association, and the National Association of Police Organizations.

Here is what the International Union of Police Associations had to say about it:

The International Union of Police Associations is proud—

Proud—

to add our name to the list of supporters of the bill addressing ''Sanctuary Cities'' titled Stop Sanctuary Policies and Protect Americans Act.

As it now stands, our officers can be held liable for sharing relevant information and honoring immigration detainers, even when they are from federal immigration officials. This legislation remedies that.

Additionally, the bill provides a financial disincentive for cities to become or remain ''sanctuary cities''. . . .

The organization also noted that this bill would help end the ''revolving door'' of criminals who ''even though convicted of felony criminal activity and deported, unlawfully return to prey upon our citizens.''

The issue before us is not truly about immigration; it is more about keeping our communities safe. Those who defend so-called sanctuary cities callously disregard how their extreme policies hurt others. The President's own DHS Secretary has used terms such as ''not acceptable'' and ''counterproductive to public safety'' when referring to sanctuary city policies. Such extreme policies can inflict almost unimaginable pain on innocent victims and their families.

As the father of three daughters, I know—I know—we can do better. I am

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

Printed on recycled paper.

calling on every colleague to put compassion before leftwing ideology today. This bill would support the deputy sheriff who puts her life on the line every day. This bill would provide hope and justice for victims and their families. So let's vote to support them, not defend extreme policies that actually hurt them.

MEASURES PLACED ON THE CALENDAR—S. 2181, S. 2182, AND S. 2183

Mr. MCCONNELL. Mr. President, I understand there are three bills at the desk due for a second reading.

The PRESIDING OFFICER. The clerk will read the bills by title for the second time.

The senior assistant legislative clerk read as follows:

A bill (S. 2181) to provide guidance and priorities for Federal Government obligations in the event that the debt limit is reached.

A bill (S. 2182) to cut, cap, and balance the Federal budget.

A bill (S. 2183) to reauthorize and reform the Export-Import Bank of the United States, and for other purposes.

Mr. MCCONNELL. In order to place the bills on the calendar under the provisions of rule XIV, I object to further proceedings en bloc.

The PRESIDING OFFICER. Objection having been heard, the bills will be placed on the calendar.

RECOGNITION OF THE MINORITY LEADER

The PRESIDING OFFICER. The Democratic leader is recognized.

SANCTUARY CITIES BILL

Mr. REID. Mr. President, I have watched over the years my Republican colleagues who are supposedly concerned about States' rights wipe them out with a speech like the one we have just heard and the legislation before this body today.

I am told and have always believed, Republicans think States and communities should have the ability to do the things they think are appropriate. Any one of these States that my friend refers to—any one of these communities—has a right at any time to change the law. This is not a Federal law they are trying to change; they are trying to change what is taking place in cities throughout the country.

So they are States' rights, my Republican colleague's own words. It certainly doesn't belie the actions they have tried to take. The Republican leader tries to make the bill before this body a political issue. It is a Donald Trump-bashing-immigrants issue.

This bill is opposed by the National Association of Chiefs of Police, it is opposed by the National Council of Mayors, and many different organizations that believe in States' rights. My friend, the Republican leader, would just make things a lot worse, and that is an understatement.

With the provisions in this bill, it is estimated it would take 15 new huge prisons just to handle the people who would be arrested—huge prisons, costing billions of dollars. It is not smart police policy. It is not smart budget policy.

THE DEBT LIMIT

Mr. REID. Mr. President, over the last 10 months, congressional Republicans have proven they are incapable of governing—at least governing productively. Instead, Republicans are governing destructively. It is hard to understand or fathom, but this seems to be what they want: destruction. It is not a word I decided to bring into the conversation today. One Republican Congressman said very recently: ''We are looking for creative destruction in how the House operates.'' This Republican Congressman said, I repeat, ''We are looking for creative destruction in how the House operates,'' and they are as good as their word in the House and sadly also in the Senate.

Time and time again, Republican leaders have brought the United States to the brink of unnecessary disaster, and sadly here we are again, facing another manufactured crisis courtesy of Republicans in Congress. This time it is a debt limit crisis. On November 3, just 2 weeks from today, our great country—the United States of America—will default on its debt unless Republicans start legislating more constructively to solve the problem. Let's be clear about what the debt limit does and doesn't mean. Adjusting the debt limit—when it is absolutely necessary, and it will be in 2 weeks—is necessary to pay this country's bills that are already due. What we face now with the debt ceiling isn't about a penny of new spending. It is not about a penny of new programs or a penny of new taxes. It is not about creating new obligations, only meeting existing ones. The debt limit is about paying what we already owe.

What are these debts? A large, large, large chunk of these is what we owe as a result of an unpaid war, a second unpaid war, and tax breaks for the rich that were unpaid for. Remember, this great theory of President Bush was that these wars would bring a new democracy to the world. Well, the invasion of Iraq was the worst foreign policy decision probably in the history of the country. Look what it has done, and it has been done at the cost of trillions of dollars of taxpayers' money, and that is part of the debt that is due.

These tax breaks for the rich. Why did the Bush administration push these tax breaks? Because it would be great for the economy. Well, it has been great for the rich people. They are getting richer, the poorer are getting poorer, and the middle class are getting squeezed. All these tax cuts were unpaid for. If we don't act, we allow the United States to default. The day of reckoning will be terrible. We will hurt American jobs, families, businesses, and the fallout will be felt around the world. If some Republicans in Congress get their way, the United States will default on this debt. What happens then? The short answer is economic catastrophe.

The former Director of the Congressional Budget Office, Douglas Holtz-Eakin, described last week what will happen if the United States defaults:

> The first thing you'll see is a market reaction. Then you've got dramatic impacts on consumer confidence, the world's melting down again and they go into an economic fetal position . . . there's just no good news there.

This wasn't some leftwing blogger; this is a man who did a good job representing this country on a bipartisan basis in the Congressional Budget Office—by the way, during a Republican administration. He said:

> The first thing you'll see is a market reaction. Then you've got dramatic impacts of consumer confidence, the world's melting down again and they go into an economic fetal position . . . there's just no good news there.

The Republican chairman of the House Ways and Means Committee, a reasonable PAUL RYAN, said as much last week:

> If the United States missed a bond payment, it would shake the confidence of the world economy. All kinds of credit would dry up: loans for small businesses, mortgages for young families. We could even go into a recession.

That is what we will face in 2 weeks if Republicans don't get their act together, and by all signs, it doesn't appear they are going to. All signs indicate that House and Senate Republicans are still not serious about dealing with the debt limit. If they were serious about paying our bills and keeping America on sound economic footing, they would not be proposing an absurd idea of having a ''partial default.'' You can't be partially pregnant; you can't have a partial default. House Republicans have engineered legislation to pick and choose which debts to pay and which to ignore.

Listen to this: Their proposed legislation is going to pay foreign creditors first, such as China, but they don't want to meet our obligations to veterans, Medicare beneficiaries, and millions of middle-class Americans. No. They want to start paying down the debt we owe to China. Think about that. The truth is this pay-China-first approach is just default by another name. This approach would lead a middle-class family into financial ruin, and just imagine what it would do to world markets. I repeat: There is no such thing as a partial default. A partial default is a default.

We can't allow the Federal Government to be delinquent in paying its debts. We have 2 weeks to get something done, and we can if the Republicans come to their senses. This unnecessary drama over paying our bills is already rattling the financial markets. The bond market has already been hurt, and we can see it.

I say to my Republican friends, especially the leaders in the House of Representatives and the U.S. Senate: Start governing in a way that is not an embarrassment to Congress and the American people.

Mr. President, please announce what we will be doing here today.

RESERVATION OF LEADER TIME

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

EXECUTIVE SESSION

NOMINATION OF ANN DONNELLY TO BE UNITED STATES DISTRICT JUDGE FOR THE EASTERN DISTRICT OF NEW YORK

The PRESIDING OFFICER. Under the previous order, the Senate will proceed to executive session to consider the following nomination, which the clerk will report.

The senior assistant legislative clerk read the nomination of Ann Donnelly, of New York, to be United States District Judge for the Eastern District of New York.

The PRESIDING OFFICER. Under the previous order, the time until 11 a.m. will be equally divided for debate in the usual form.

The assistant Democratic leader.

REFUGEE CRISIS IN GREECE, NOMINATION OF GAYLE SMITH, AND UKRAINE

Mr. DURBIN. Mr. President, I had the privilege of joining Senators SHAHEEN, KLOBUCHAR, and WARREN during the recess that just concluded to travel to Europe to assess the refugee flow that is spilling into Greece and ongoing Russian aggression during our visit to Ukraine.

I will start with the visit to one of our most important NATO European allies, Greece. Greece is struggling, as we all know, with its own economic challenges, but now it is facing an overwhelming flow of refugees across its border.

Almost half a million refugees have flown into Greece just this year. The bulk of the refugees come from across the Aegean Sea from Turkey. They are fleeing war and economic instability in the region. Most are from Syria, but there are many others from Afghanistan, Iraq, and other countries in peril. Many are middle-class families who are simply exhausted from years of horrific war in Syria.

I met many of them and had a chance to speak to them. Their stories are heartbreaking. They are fleeing with their children and whatever they can carry. Their destination is uncertain, but they know they can't stay in the camps or in Syria. They are the victims of smugglers and exploitation. Some of these desperate people are charged 1,000 Euros just to cross a 2-mile stretch of ocean between Turkey and Greece.

We were on the island of Lesbos, and those who were able to watch ''60 Minutes'' this week saw a presentation of what is happening on that small island of about 80,000 people where more than 400,000 refugees have come through in the last several weeks. Many of these refugees are unaccompanied children.

At one of the camps, I met a young man who said he was 17—probably 15—who had come across that stretch of water with his 8-year-old sister. Think for a moment what that family must have gone through in deciding that it was safer for this 15-year-old to take his 8-year-old sister and try to find their way to a safe place in Europe rather than stay in war-torn Syria. That is the reality of many of these refugees and the plight that they face.

On this island of Lesbos, 2,000 refugees are arriving every single day. The Greek Coast Guard showed us stacks of discarded rubber rafts. These rubber rafts are made to hold about 20 people as they cross this 3-mile stretch of ocean. They packed them with over 50 people. They charge 1,000 Euros for each adult and 500 Euros for each child.

We saw these rafts stacked up and piles of life preservers. Some of them are the types of life preservers and jackets that you might expect, but others are ridiculous. Some of them are literally pool toys, and they say so. They have written right on them that they are not to be used as life preservers. These pool toys are strapped to those little kids who are put in these rafts that come across that stretch of ocean. There were rows upon rows of cheap outboard motors that were used to propel these rafts across the straits.

Incidentally, the smugglers picked someone in the raft and told them that they were in charge. They would ask if they knew how to operate the motor. If they didn't know how to operate it, they would show them how to use it and point them in the right direction. The refugees would then head out in the hope that they would make it across safely, and many times they didn't.

Despite Greece's economic hardship, I was impressed with how the Greek people were handling this refugee crisis. Processing registration centers had been established, and many refugees were quickly on their way to resettlement in Europe.

I mentioned the 15-year-old with his 8-year-old sister. I ran into four others who spoke English, and all of them were college graduates in their 20s. One of them was a premed student who said: We just couldn't live any longer with war in Syria. We were ready to risk our lives to find a safer place.

The mayor of Lesbos has been generous and thoughtful in addressing the suffering. He told me he often thought he was handling a ticking time bomb with this refugee crisis. Instead, this island has become an example of what the rest of the world can do.

In Athens, we visited with an impressive NGO known as Praksis that is giving unaccompanied minors a safe, nurturing place to stay while they attempt to place them with families.

The United States leads the world in financial assistance for this Syrian refugee effort, but we have a moral obligation to do that and more. I have called on the administration to accept 100,000 Syrian refugees. I am a cosponsor of the emergency supplemental bill addressing refugee assistance, recently introduced by Senators GRAHAM and LEAHY.

Allow me to put the 100,000 number in perspective. Germany has agreed to accept 800,000 of these Syrian refugees. It is estimated that there are 4 million total. The United States accepted 750,000 Vietnamese refugees and over 500,000 Cuban refugees after the Castro regime took over. Those Cuban refugees included the fathers of two sitting U.S. Senators, one of whom is running for President of the United States. We accepted over 200,000 Soviet Jews who were being persecuted in that country. We have accepted refugees from Somalia and from different places around the world, such as Bosnia. We have assimilated them into America, and we can do it again.

When we go through this process of accepting refugees, we carefully check their backgrounds to make sure that they are not a threat to the United States or anybody who lives here. I think we should continue to do that, but the fact that only 1,700 have made it to our Nation in the last 4 years tells us that we need to do more.

I will continue to be a strong advocate for humanitarian safe zones in Syria so the people there can have a safe place to be treated for their illnesses and to at least live until this war comes to an end.

Let me say something else. It is embarrassing for me to stand before the Senate and note that on our Executive Calendar, which is on the desks of Senators, there includes one nominee, Gayle Smith, who has been nominated to be administrator of the United States Agency for International Development. She has been sitting on this calendar since July 29 of this year.

The USAID, which she seeks to head, is the premier frontline agency for helping refugees. Yet this good woman with a lifetime of experience is being held up in the Senate for entirely political reasons. There are no objections to her personally, and there are no objections to her background.

One Senator is holding up her nomination because the Senator stated publicly that he objects to the President's Iran nuclear agreement. Gayle Smith had nothing to do with that. The USAID had nothing to do with that. Shouldn't we appoint this good person to manage this agency to deal with this international refugee crisis?

While we are at it, they are asking that Thomas Melia of Maryland be the assistant administrator. Wouldn't we want competent management when we are talking about billions of American

tax dollars being spent wisely in this humanitarian effort? Yet they languish on this calendar.

If there are objections to these nominees, state them. If not, approve them.

After Greece, we had a visit to Ukraine. I believe what is happening there is deeply important to us in the United States, and I am committed to seeing that Ukraine succeed as a Democratic sovereign nation. It is hard to describe what has happened there in a year and a half. A shamefully corrupt regime which is deeply influenced by Russia was rejected by the Ukrainian people. As the country tried to get back on its feet and build a more transparent and Democratic future, Russia and Vladimir Putin staged an invasion first by taking over Crimea and then by invading eastern Ukraine.

The Russians have turned eastern Ukraine into a dysfunctional, grim, and abandoned wasteland, somehow under the illusion that it would be the new Russia. More than a million people have been displaced in eastern Ukraine and thousands have been killed. The captured land was even used as a base to shoot down a civilian airliner, killing hundreds. A recent Dutch investigation showed that this was done with Russian weaponry. If only President Putin would try to help with the investigation of the Malaysian plane that was shot down instead of nakedly blocking the effort of the U.N. Security Council, we would have even more information about this horrible tragedy.

Despite agreeing in Minsk to a pullback of heavy weapons, exchange of prisoners, and return of border control in the east, Russia has dragged its feet on every term of the agreement, incorrectly hoping that the world will not notice. We notice.

Yet amid all this transparent and barbaric effort to undermine Ukraine, the country has found a new unity and determination. It has taken on significant reforms. During my visit with my fellow Senators, I was struck by how many dedicated Ukrainians are working for a better future. They are now members of Parliament and local officials coming right out of the Maidan demonstration. They are giving everything they can for the future of their country.

I have been a strong supporter of President Obama's efforts to support Ukraine to train and equip its military and provide significant assistance for their courageous effort. As the world's attention is distracted to many other challenges, let's not lose sight of the ongoing struggle in Ukraine. The United States and Europe must remain united on sanctions against Russia as long as it continues to invade and occupy a sovereign nation like Ukraine.

I will conclude by recognizing the many dedicated Foreign Service officers working in our embassies that we meet with on our trips. They are on the frontlines of American leadership and generosity. Ambassador Geoffrey Pyatt in Ukraine and Ambassador David Pearce in Greece are two we worked with during our recent visit.

As the Republicans threaten government shutdown after government shutdown, let us not forget that these men and women and many like them literally risk their lives every single day standing up and representing the United States around the world.

Mr. President, I yield the floor.

The PRESIDING OFFICER. The Senator from Louisiana.

STOP SANCTUARY POLICIES AND PROTECT AMERICANS BILL

Mr. VITTER. Mr. President, I rise again in strong support of the Stop Sanctuary Policies and Protect Americans Act, which we will be voting on later today. I was here on the floor yesterday laying out the strong case in support of that, talking to many colleagues before this vote today, as I have been for the past several days.

Today I rise to focus on some arguments from the other side that are erroneous and misleading, quite frankly, and to debunk those arguments so everyone has the full, true, and clear picture of why this legislation is so needed.

First, I have heard a few of my colleagues talk about the need for Federal and local authorities to do a better job of working together. For instance, Senator DURBIN, who just left the floor, said: ''Federal and local authorities must do a better job of communicating and coordinating so that undocumented immigrants with serious criminal records are detained and deported, period.''

Similarly, Senator FEINSTEIN said: ''It is very clear to me that we have to improve cooperation between local, State, and Federal law enforcement.''

Let me say that I completely agree with them, and they are laying out a strong case for this legislation, not against it, because we need to do something about the cause of the noncooperation, the obstacle between that full cooperation, which absolutely needs to happen every day. Simply wishing for a better outcome isn't going to make it happen.

The fact is, there are dozens of sanctuary cities—jurisdictions that have those policies—that were cooperating in the past and that want to cooperate, but they have been faced with lawsuits from the ACLU and others and court decisions wherein local law enforcement officials could be held liable for violating an individual's constitutional rights simply for honoring a detainer request from ICE. That is ridiculous. That is an abusive threat. Our legislation on the floor today is going to remove that threat.

The Stop Sanctuary Policies and Protect Americans Act allows for that cooperation between local and Federal authorities to resume again because section 4 of the bill will facilitate State and local compliance with the ICE detainer and remove that onerous and unreasonable threat. Cooperation has been stifled by lawsuits aimed at bullying local law enforcement, and this bill will grant local law enforcement the authority to clearly comply with ICE detainers without threat of liability. It will protect them from that liability for simply complying with ICE detainers.

I will remind my colleagues that it will do nothing to infringe on an individual's civil or constitutional rights. They still have the same ability to pursue those against ICE or anyone else they choose.

That is why this legislation is supported by people who know something about what needs to happen for local and Federal authorities to cooperate. Who am I talking about? The Federal Law Enforcement Officers Association—they know what they are talking about. The International Union of Police Associations—they live it every day. The National Association of Police Organizations and the National Sheriffs' Association—don't my colleagues think they know what is needed on the ground? They do. And because they do, they strongly support this legislation.

Second, some colleagues on the other side argue that this bill won't do anything; instead, we need so-called comprehensive immigration reform such as the Gang of 8 bill. But the Gang of 8 bill that my colleagues are pushing—1,200 pages long when it passed the Senate—didn't do anything to resolve this issue of sanctuary cities. It didn't do anything to change the abusive lawsuits I am speaking about. It didn't do anything to encourage Federal and local authorities to cooperate in real time—absolutely nothing. That is just the fact, once we read the 1,200 pages. All the Gang of 8 bill does is lead with a big amnesty—an amnesty overnight—for about 11 million illegal immigrants in our country today. So that comprehensive immigration reform bill—the Gang of 8 bill or whatever we want to call it—does nothing in this area that is so crucial to fix, does nothing about sanctuary cities, does nothing to remove these abusive lawsuits as obstacles to the clear and full cooperation between Federal, State, and local authorities, which even folks on the other side of the bill admit needs to happen and is a problem right now.

There are lots of myths about our bill versus the facts.

With that in mind, I ask unanimous consent to have printed in the RECORD a myth v. fact sheet that lays out clearly the myths, the arguments made against this legislation, and the real facts of the Stop Sanctuary Policies and Protect Americans Act, S. 2146.

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

MYTH V. FACT—STOP SANCTUARY POLICIES ACT (S.2146)

1. S.2146 does not punish illegal immigrants who come forward to report crimes.

Myth: Under S.2146, ''reporting crimes or otherwise interacting with law enforcement could lead to immigration detention and deportation.''[1]

Fact: S.2146 provides that if a jurisdiction has a policy that local law enforcement will not inquire about the immigration status of crime victims or witnesses, such jurisdiction will not be deemed a sanctuary jurisdiction and will not lose any federal funds. See section 3(e).

2. S.2146 does not require local law enforcement to carry out federal immigration responsibilities.

Myth: S.2146 would ''require[e] state and local law enforcement to carry out the federal government's immigration enforcement responsibilities,'' and thus ''the federal government would be substituting its judgment for the judgment of state and local law enforcement agencies.''[2]

Fact: The bill does not require local law enforcement ''to carry out federal immigration responsibilities.'' Removing illegal immigrants remains the exclusive province of the federal government. The bill simply withholds certain federal funds from jurisdictions that prohibit their local law enforcement officers from cooperating with federal officials in the limited circumstance of honoring an immigration detainer.

It is politicians in sanctuary jurisdictions who, by tying the hands of local law enforcement, are ''substituting [their] judgment for the judgment of state and local law enforcement.''

3. S.2146 is necessary to keep dangerous criminals off of the streets.

Myth: ''Congress should focus on overdue reforms of the broken immigration system to allow state and local law enforcement to focus their resources on true threats—dangerous criminals and criminal organizations.''[3]

Fact: Sanctuary cities are the ones preventing local law enforcement from focusing on dangerous criminals and criminal organizations—by forbidding local law enforcement officers from holding such criminals.

The illegal immigrant who killed Kate Steinle explained that he chose to live in San Francisco because it was a sanctuary city, and he knew San Francisco would not take action against him He was right. Three months before Kate's death, the federal government asked San Francisco officials to hold him, but San Francisco refused.

4. S.2146 does not force the U.S. to bear liability for unconstitutional actions by local law enforcement.

Myth: S.2146 includes ''provisions requiring DHS to absorb all liability in lawsuits brought by individuals unlawfully detained in violation of the Fourth Amendment.''[4]

Fact: If a lawsuit alleges that a local officer knowingly violated Fourth Amendment or other constitutional rights, under S.2146, the individual officer, not the federal government, will bear all liability. See section 4(c).

For some lawsuits, the U.S. will be substituted as defendant—specifically, suits alleging that that the immigration detainer should not have been issued. But such a claim could already be brought against the U.S. under existing law; thus, S.2146 does not create a new source of liability for the federal government. S.2146 simply provides that if the federal government made the error, the federal government should be the defendant.

5. S.2146 is fully consistent with the Fourth Amendment and preserves individuals' rights to sue for constitutional violations.

Myth: ''The Fourth Amendment provides that the government cannot hold anyone in jail without getting a warrant or the approval of a judge.''[5]

Fact: The Constitution requires probable cause to detain an individual, which can be established by a judicial a warrant issued before the arrest or by a demonstration of probable cause after the arrest. Otherwise police could never arrest someone whom they see committing a crime.

S.2146 does not alter the requirement for probable cause. In fact, S.2146 explicitly preserves an individual's ability to sue if he or she is held without probable cause or has suffered any other violation of a constitutional right.

ENDNOTES

1. Email from Lutheran Immigration and Refugee Service (Oct. 19, 2015).
2. Letter from Law Enforcement Immigration Task Force (Oct. 15, 2015).
3. Letter from Law Enforcement Immigration Task Force (Oct. 15, 2015).
4. Letter from ACLU (Oct. 19, 2015).
5. Letter from ACLU (Oct. 19, 2015).

Mr. VITTER. Mr. President, let me highlight the two biggest ones. The first one is that our legislation would somehow punish and make it more difficult for illegal persons to report crimes and cooperate with local law enforcement. That is a pure myth. What is the fact? Well, read the bill, as the American people suggest. Read the bill. Our bill, S. 2146, specifically provides that if a jurisdiction has a policy that local law enforcement will not inquire about the immigration status of crime victims or witnesses, such jurisdiction will not be deemed a sanctuary jurisdiction and it will not lose Federal funds over that. So that argument is simply a myth.

The second argument often made is that somehow this legislation is requiring local law enforcement to carry out Federal immigration responsibilities. Again, that is a pure myth, a purely erroneous argument, and if we read the bill, S. 2146, we will see it is simply not true. The bill does not require local law enforcement ''to carry out Federal immigration responsibilities'' in any way, shape, or form. Removing illegal immigrants remains the exclusive province of the Federal Government. The bill simply withholds certain Federal funds from jurisdictions that prohibit exactly the cooperation that our opponents on the other side say is so necessary and correctly say is so necessary. So that, again, is the fact versus the myth that is being propagated.

Again, we have several myths versus facts as part of the record, and I urge everyone, starting with our colleagues, Democrats and Republicans, to study it carefully.

This is an important issue. Sanctuary cities are a real problem, and we need to fix that problem to move forward. So I urge my colleagues to look carefully at this issue of what is driving these sanctuary cities policies. Our legislation will take up those drivers, those obstacles, will solve those problems, and will result in the cooperation at all levels of law enforcement that we desperately need.

I urge my colleagues to vote yes later today so we can push forward with this important and critical legislation.

Mr. LEAHY. Mr. President, today, we will finally vote on the nomination of Judge Ann Donnelly to be a Federal district judge in the Eastern District of New York. She was first nominated for this judicial emergency vacancy nearly a year ago, back in November 2014. She was voted out of the Judiciary Committee by unanimous voice vote over 4 months ago on June 4, but since then she has been blocked from receiving a vote on the Senate floor. Senator SCHUMER has twice sought to secure a vote for Judge Donnelly through unanimous consent requests in July and September, but was blocked by Republicans both times. No substantive reason was given for this obstruction, which is hurting both our justice system and the people who seek justice in those courts.

Judge Donnelly is not the only New York nominee ready for a vote today on the Executive Calendar. LaShann Hall, a partner at a prominent national law firm, was nominated to the other judicial emergency vacancy in the Eastern District of New York last November as well. She was voted out of the Judiciary Committee by unanimous voice vote at the same time as Judge Donnelly, and she is still awaiting a vote.

Also waiting for a vote is Lawrence Vilardo, who has been nominated to the vacancy in the Western District of New York in Buffalo. The Western District of New York has one of the busiest caseloads in the country and handles more criminal cases than Washington, DC, Boston, or Cleveland; yet there is not a single active Federal judge in that district, and the court is staying afloat only through the voluntary efforts of two judges on senior status who are hearing cases in their retirement. Despite these circumstances, Republicans continue to hold Mr. Vilardo's nomination up as well. There is no good reason why these two other noncontroversial New York nominees could not be confirmed today. The same goes for the rest of the noncontroversial judicial nominees on the Executive Calendar.

In the Judiciary Committee, I have continued to work with Chairman GRASSLEY to hold hearings on judicial nominees. We will hold a hearing tomorrow for four more judicial nominees. But the pattern we have seen over the last 9 months is that, once nominees are voted out of committee and awaiting confirmation on the floor, the Republican leadership refuses to schedule votes. So far this year, we have only confirmed seven judges. That is not even one judge per month. Some Republicans claim that this is reasonable, but by any measure, it is not. By this same point in 2007, when I was chairman of the Judiciary Committee and we had a Republican President, the Senate had already confirmed 33 judges. At this current rate, by the end of the year, the Senate will have confirmed the fewest number of judges in more than a half century.

This pattern is especially egregious in light of the rising number of judicial vacancies. In fact, as a direct result of Republican obstruction, vacancies have

increased by more than 50 percent, from 43 to 67. That means there are not enough judges to handle the overwhelming number of cases in many of our Federal courtrooms. Additionally, the number of Federal court vacancies deemed to be ''judicial emergencies'' by the nonpartisan Administrative Office of the U.S. Courts has increased by 158 percent since the beginning of the year. There are now 30 judicial emergency vacancies that are affecting communities across the country.

The Leadership Conference on Civil and Human Rights recently issued a memorandum documenting the real life impact of the Senate Republicans' obstruction on the judicial confirmation process. Three States where communities are most hurt are Texas, Alabama, and Florida. Texas, for example, has nine judicial vacancies—with seven of them deemed to be judicial emergencies. Incredibly, one of the district court positions has been vacant for over 4 years, and a fifth circuit position in Texas has been vacant for more than 3 years. The memorandum reports that, in the Eastern District of Texas, the delays caused by the vacancy in that court has placed greater pressure on criminal defendants to forego trials and simply plead guilty to avoid uncertain and lengthy pretrial detentions. That is not justice.

Similarly, Alabama has five current vacancies that remain unfilled, and Florida has three. These rising vacancies are leading to an unsustainable situation in too many states. As Chief Judge Federico Moreno of the Southern District of Florida noted, ''It's like an emergency room in a hospital. The judges are used to it and people come in and out and get good treatment. But the question is, can you sustain it? Eventually you burn out.''

I urge the majority leader to schedule votes for the 14 other consensus judicial nominees on the Executive Calendar without further delay. If the Republican obstruction continues and if home State Senators cannot persuade the majority leader to schedule a vote for their nominees soon, then it is unlikely that even highly qualified nominees with Republican support will be confirmed by the end of the year. These are nominees that members of the leader's own party want confirmed. Let us work together to confirm nominees and help restore our third branch to full strength.

Shortly we will begin voting on Judge Ann Donnelly to fill a judicial emergency vacancy in the Federal District Court for the Eastern District of New York. Since September 2014, she has served as a judge on the New York County Supreme Court. Judge Donnelly previously presided on the Kings County Supreme Court from 2013 to 2014 and in the Bronx County Supreme Court from 2009 to 2013. Prior to becoming a judge, she worked at the New York County District Attorney's Office for 25 years as an assistant district attorney, senior trial counsel, and as chief of the Family Violence Child Abuse Bureau. She has the support of her two home State Senators, Senator SCHUMER and Senator GILLIBRAND. She was voted out of the Judiciary Committee by unanimous voice vote on June 4, 2015. I will vote to support her nomination.

Mr. VITTER. 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.

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

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

The PRESIDING OFFICER. Under the previous order, the question is, Will the Senate advise and consent to the nomination of Ann Donnelly, of New York, to be United States District Judge for the Eastern District of New York?

Mr. FRANKEN. Mr. 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 South Carolina (Mr. GRAHAM) and the Senator from Florida (Mr. RUBIO).

Mr. DURBIN. I announce that the Senator from New Hampshire (Mrs. SHAHEEN) is necessarily absent.

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

The result was announced—yeas 95, nays 2, as follows:

[Rollcall Vote No. 279 Ex.]

YEAS—95

Alexander	Fischer	Murphy
Ayotte	Flake	Murray
Baldwin	Franken	Nelson
Barrasso	Gardner	Paul
Bennet	Gillibrand	Perdue
Blumenthal	Grassley	Peters
Booker	Hatch	Portman
Boozman	Heinrich	Reed
Boxer	Heitkamp	Reid
Brown	Heller	Risch
Burr	Hirono	Roberts
Cantwell	Hoeven	Rounds
Capito	Inhofe	Sanders
Cardin	Isakson	Sasse
Carper	Johnson	Schatz
Casey	Kaine	Schumer
Cassidy	King	Scott
Coats	Kirk	Sessions
Cochran	Klobuchar	Shelby
Collins	Lankford	Stabenow
Coons	Leahy	Tester
Corker	Lee	Thune
Cornyn	Manchin	Tillis
Cotton	Markey	Toomey
Crapo	McCain	Udall
Cruz	McCaskill	Vitter
Daines	McConnell	Warner
Donnelly	Menendez	Warren
Durbin	Merkley	Whitehouse
Enzi	Mikulski	Wicker
Ernst	Moran	Wyden
Feinstein	Murkowski	

NAYS—2

Blunt Sullivan

NOT VOTING—3

Graham Rubio Shaheen

The nomination was confirmed.

The PRESIDING OFFICER. Under the previous order, the motion to reconsider is considered made and laid upon the table, and the President will be immediately notified of the Senate's action.

LEGISLATIVE SESSION

The PRESIDING OFFICER. Under the previous order, the Senate will resume legislative session.

STOP SANCTUARY POLICIES AND PROTECT AMERICANS ACT—MOTION TO PROCEED

The PRESIDING OFFICER. Under the previous order, the Senate will resume consideration of the motion to proceed to S. 2146, which the clerk shall now report.

The legislative clerk read as follows:

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.

The Senator from Texas.

Mr. CRUZ. Mr. President, the American people have demanded for years that the Federal Government faithfully enforce our Nation's immigration laws. Americans are tired of seeing their laws flouted and their communities plagued by the horrible crimes that typically accompany illegal immigration. But for too long, the pleas of the American people on this issue have gone unheeded here in Washington.

See, when it comes to the problem of illegal immigration, the political class and the business class—our Nation's elites—are of one mind. They promise robust enforcement at some point in the future but only on the condition that the American people accept a pathway to citizenship now for the millions of illegal immigrants who are already in this country.

Not wanting to be swindled, the American people wisely rejected this deal, which the Washington class calls ''comprehensive immigration reform.'' Of course, the elites don't like this one bit. So instead, they have taken matters into their own hands. They bend or ignore the law to make it more difficult for immigration enforcement officers to do their job.

We have seen this repeatedly with the Obama administration. President Obama has illegally granted amnesty to millions of illegal immigrants with no statutory authorization whatsoever, even though, before his reelection, the President assured the American people he couldn't do so without an act of Congress. As President Obama said, when asked whether he could grant amnesty, ''I am not an emperor.''

Well, I agree with President Obama. But yet, just a few months after saying he couldn't do this because he was not an emperor, apparently he discovered he was an emperor, because he did precisely what he acknowledged he lacked the constitutional authority to do.

Although the administration today claims to be focusing its resources on deporting illegal immigrants with criminal records, it has adopted a policy where many illegal immigrants that the administration deems to be low-priority criminals will not be detained and deported but will be released back into our communities.

Remarkably, in the year 2013 the Obama administration released from detention roughly 36,000 convicted criminal aliens who were actually awaiting the outcome of deportation proceedings. These criminal aliens were responsible for 193 homicide convictions. They were responsible for 426 sexual assault convictions, 303 kidnapping convictions, 1,075 aggravated assault convictions, and 16,070 drunk driving convictions. All of this was on top of the additional 68,000 illegal immigrants with criminal convictions that the Federal Government encountered in 2013 but never took into custody for deportation. Dwell on those numbers for a moment.

In 1 year, the Obama administration releases over 104,000 criminal illegal aliens, people who have come into this country illegally who have additional criminal convictions—murderers, rapists, thieves, drunk drivers.

One wonders what the administration says to the mother of a child lost to a murderer released by the Obama administration because they will not enforce the laws. One wonders what the Obama administration says to the child of a man killed by a drunk driver released by the Obama administration because they will not enforce our immigration laws.

While this administration's refusal to enforce the laws is bad enough, the scandalously poor enforcement of our immigration laws is made much, much worse by the lawless actions of the roughly 340 so-called sanctuary jurisdictions across the country. Although these jurisdictions are more than happy—eager, even—to take Federal taxpayer dollars, they go out of their way to obstruct and impede Federal immigration enforcement by adopting policies that prohibit their law enforcement officers from cooperating with Federal officers. Some of the jurisdictions even refuse to honor requests from the Federal Government to temporarily hold a criminal alien until Federal officers can take custody of the individual. Not only are these sanctuary policies an affront to the rule of law, but they are extremely dangerous.

According to a recent study by the Center for Immigration Studies, between January 1 and September 30, 2014—just a 9-month period—sanctuary jurisdictions released 9,295 alien offenders who the Federal Government was seeking to deport. That is roughly 1,000 offenders a month that sanctuary jurisdictions released to the people. Now, of those 9,295, 62 percent had prior criminal histories or other public safety issues. Amazingly, to underscore just how dangerous this is to the citizenry, 2,320 of those criminal offenders were rearrested within the 9-month period for committing new crimes after they had already been released by the sanctuary jurisdiction. If that doesn't embody lawlessness, it is difficult to imagine what does—jurisdictions that are releasing over and over criminal illegal aliens, many of them violent criminal illegal aliens, and exposing the citizens who live at home to additional public safety risk, to additional terrorist risk.

This same study found that the Federal Government was unable to reapprehend the vast majority of the alien offenders released by the sanctuary jurisdictions—69 percent as of last year. Even Homeland Security Secretary Jeh Johnson has admitted that these sanctuary policies are ''unacceptable.'' ''It is counterproductive to public safety,'' he said, ''to have this level of resistance to working with our immigration enforcement personnel.''

I am thrilled to hear the Secretary of Homeland Security say so out loud. I assume that means that the Obama administration will be supporting the legislation before this body. After all, the Secretary of Homeland Security says it is ''unacceptable,'' and that ''it is counterproductive to public safety.'' Yet, sadly, the Obama administration is not supporting the legislation before this body.

Indeed, it has taken the tragic and terrible death of Kate Steinle to galvanize action here in Washington. Kate died in the arms of her father on a San Francisco pier after being fatally shot by an illegal alien who had several felony convictions and had been deported from the United States multiple times. Her death is heartbreaking.

In the Senate Judiciary Committee we had the opportunity to hear from Kate Steinle's family. The heartbreak is even more appalling because Kate's killer had been released from custody and not turned over to the Federal Government to be deported because of San Francisco's sanctuary policy.

The city of San Francisco is proudly a sanctuary city. They say to illegal immigrants across the country and across the world: Come to San Francisco. We will protect you from Federal immigration laws. We, the elected democratic leaders of this city, welcome illegal immigrants, including violent criminal illegal immigrants such as the murderer who took Kate Steinle's life.

These policies are inexcusable. They are a threat to the public safety of the American people, and they need to end. That is why I am proud to be one of the original cosponsors of the Stop Sanctuary Policies and Protect Americans Act, which strips certain Federal funds, especially community development block grants, from jurisdictions that maintain these lawless policies. If these jurisdictions insist on making it more difficult to remove criminal aliens from our communities, then these Federal dollars should go instead to jurisdictions that will actually cooperate with the Federal Government, that are willing to enforce the law rather than aid and abet the criminals. It makes no sense to continue sending Federal money to local governments that intentionally make it more difficult and costly for the Federal Government to do its job.

But this bill doesn't just address sanctuary jurisdictions. It also addresses the problem of illegal immigrants who, like Kate Steinle's killer, are deported but illegally reenter the country, which is a felony. This class of illegal aliens has a special disregard and disdain for our Nation's laws, and too often these offenders also have serious rap sheets.

In 2012, just over a quarter of the illegal aliens apprehended by Border Patrol had prior deportation orders. That is an astounding 99,420 illegal aliens. Of the illegal reentry offenders who were actually prosecuted in fiscal year 2014—that is just 16,556 offenders—a fraction of those committed a felony. The majority of those who were prosecuted had extensive or recent criminal histories, and many were dangerous criminals. Even though the majority of offenders had serious criminal records, the average prison sentence was just 17 months, down from an average of 22 months in 2008.

In fact, more than a quarter of illegal reentry offenders received a sentence below the guidelines range because the government sponsored the low sentence. Because we are failing to adequately deter illegal aliens who have already been deported from illegally reentering the country, I introduced Kate's Law in the Senate.

I wish to thank Senators VITTER and GRASSLEY for working with me to incorporate elements of Kate's Law into this bill. I also wish to recognize and thank all of the original cosponsors who joined me in this bill—Senators BARRASSO, CORNYN, ISAKSON, JOHNSON, PERDUE, RUBIO, SULLIVAN, and TOOMEY.

Because of this bill, any illegal alien who illegally reenters the United States and has a prior aggravated felony conviction or two prior illegal reentry convictions will face a mandatory sentence of 5 years in prison. We must send the message that defiance of our laws will no longer be tolerated, whether it is by the sanctuary cities themselves or by the illegal reentry offenders who they harbor.

The problem of illegal immigration in this country will never be solved until we demonstrate to the American people that we are serious about securing the border and enforcing our immigration laws and until we have a President who is willing to and, in fact, committed to actually enforcing the laws and securing the borders.

This bill is just a small step, but at least it is a step in the right direction. Yet there will be two consequences from the vote this afternoon. First, it will be an opportunity for our friends on the Democratic side of the aisle to declare to the country on whose side they stand.

When they are campaigning for reelection, more than a few Democratic Senators tell the voters they support securing the borders. More than a few Democratic Senators tell the voters: Of course we shouldn't be releasing criminal illegal aliens. More than a few Democratic Senators claim to have no responsibility for the 104,000 criminal illegal aliens released by the Obama administration in the year 2013.

These Senators claim to have no responsibility for the murder of Kate Steinle, invited to San Francisco by that city's sanctuary city policy. This vote today will be a moment of clarity. No Democratic Senator will be able to go and tell his or her constituents: I oppose sanctuary cities. I support securing the border if they vote today in favor of sending Federal taxpayer funds to subsidize the lawlessness of sanctuary cities.

The Senate Judiciary Committee heard testimony from families who had lost loved ones to violent criminal illegal aliens—one after the other after the other. We heard about children who were sexually abused and murdered by violent illegal aliens. We heard from family members who have lost loved ones to drunk drivers illegally in this country.

During the hearing, I asked the senior Obama administration official for immigration enforcement how she could look into the eyes of those family members and justify releasing murderers, rapists, and drunk drivers over and over and over again.

Indeed, at that hearing I asked the head of immigration enforcement for the Obama administration: How many murderers did the Obama administration release this week? Her answer: I don't know. I asked her: How many rapists did the Obama administration release this week? Her answer: I don't know. How many drunk drivers? I don't know.

None of us should be satisfied with that answer or with a President and administration that refuse to enforce the laws and are willfully and repeatedly releasing violent criminal illegal aliens into our communities and endangering the lives of our families and children.

This vote today is a simple decision for every Democratic Senator: With whom do you stand? Do you stand with the violent criminal illegal aliens who are being released over and over again? Because mind you, a vote no is to say the next time the next murderer—like Kate Steinle's murderer—comes in, we should not enforce the laws, and we shouldn't have a mandatory 5-year prison sentence. Instead, we should continue sanctuary cities that welcome and embrace him until perhaps it is our family members who lose their lives.

It is my hope that in this moment of clarity the Democratic members of this body will decide they stand with the American people and not with the violent criminal illegal aliens.

It is worth noting, by the way, the standard rhetorical device that so many Democratic Senators use is to say: Well, not all immigrants are criminals. Well, of course they are not. I am the son of an immigrant who came legally to this country 58 years ago. We are a nation of immigrants, of men and women fleeing oppression and seeking freedom, but this bill doesn't deal with all immigrants. It deals with one specific subset of immigrants: criminal illegal aliens. It deals with those who come to this country illegally and also have additional criminal convictions, whether it is homicide, sexual assault, kidnapping, battery, or drunk driving. If it is the Democrats' position for partisan reasons that they would rather stand with violent criminal illegal aliens, that is a sad testament on where one of the two major political parties in this country stands today. I suspect the voters who elect them would be more than a little surprised at how that jibes with the rhetoric they use on the campaign trail.

If, as many observers predict, Democratic Senators choose to value partisan loyalty to the Obama White House over protecting the lives of the children who will be murdered by violent criminal illegal aliens in sanctuary cities if this body does not act, and if they vote on a party-line vote, as many observers have predicted, that will provide a moment of clarity. I will also suggest that it underscores the need for Republican leadership to bring this issue up again—and not in the context where Democrats can blithely block it and obstruct any meaningful reforms to protect our safety, secure the border, enforce the law, and stop violent illegal criminal aliens from threatening our safety—in the context of a must-pass bill and attach it to legislation that will actually pass in law.

I am very glad we are voting on this bill this week. That is a good and positive step. It is one of the few things in the last 10 months we have voted on that actually responds to the concerns of the men and women who elected us.

I salute leadership for bringing up this vote, but if a party-line vote blocks it, then the next step is not simply to have a vote. The next step is to attach this legislation to must-pass legislation and to actually fix the problem. Leadership loves to speak of what they call governing, and in Washington governing is always set at least an octave lower. Well, when it comes to stopping sanctuary cities and protecting our safety, we need some governing. We need to actually fix the problem rather than have a show vote.

My first entreaty is to my Democratic friends across the aisle. Regardless of areas where we differ on partisan politics, this should be an easy vote. Do you stand with the men and women of your State or do you stand with violent criminal illegal aliens? We will find out in just a couple of hours.

My second entreaty is to Republican leadership. If Democrats are partisans first rather than protecting the men and women they represent, then it is up to Republican leadership to attach this to a must-pass bill and actually pass it into law and solve the problem—not to talk about it, but to do it. It is my hope that is what all of us do together.

I yield the floor.

The PRESIDING OFFICER (Mr. FLAKE). The Senator from New Jersey.

Mr. MENENDEZ. Mr. President, I rise today to speak out against a bill that is misguided, stands against everything that America represents, and suggests that it will protect Americans when, in fact, it will protect Americans less.

From our founding, our principles have been guided by core values of equality, fairness, freedom, and tolerance, and in turn, we have honored the many ways that immigrants have contributed to this country since its inception. Yet the other side of the aisle is once again engaged in a stubborn, relentless, and shameful assault against immigrants.

As the son of immigrants myself, I find it hard not to take offense at the anti-immigrant rhetoric we are hearing from their Presidential candidates. It is unacceptable, deplorable, and should be renounced by every American. We are witnessing the most overtly nativist, xenophobic campaign in modern U.S. history. We have hit a new low with the extraordinarily hateful rhetoric that diminishes immigrants' contributions to American history and particularly demonizes the Latino community by labeling Mexican immigrants as rapists and criminals.

The Republican leading in the polls actually launched his Presidential candidacy by attacking immigrants, saying:

> They're bringing drugs. They're bringing crime. They're rapists.

Please spare me. It is senseless and false. Yet some of my Senate colleagues have decided to jump on the GOP's fearmongering bandwagon, seeking to blindly stamp millions of hardworking, law-abiding immigrant families as criminals and rapists, and that is why we are here today. That anti-immigrant rhetoric has made its way to the Senate floor courtesy of Donald Trump and some Republicans eager to capitalize on this rhetoric for their own political gain.

This is nothing more than another offensive anti-immigrant bill, another effort to demonize those who risk everything for a better life for themselves and their children, those who were left with no choice but to flee persecution and violence or else face a certain death. That is what we are debating here today. Those are the individuals this legislation seeks to brand as criminals.

This bill does nothing more than instigate fear and divide our Nation. Supporters of this bill may say that it is in response to a tragedy such as what happened in San Francisco, and what happened in San Francisco was a tragedy. Such tragedies will not be prevented by this legislation but by real immigration reform. I am happy to have that debate—a real debate, an honest and compassionate debate, a debate the country deserves—but that is not what is happening in this bill.

The title of the bill asserts that it will protect Americans. Well, to be clear, this bill will not protect Americans because it second guesses decisions made by local law enforcement around the country about how to best police their own communities and ensure public safety.

What is worse, this bill mandates local law enforcement to take on Federal immigration enforcement duties by threatening to strip away funding from as many as 300 local jurisdictions, from programs such as the community development block grant, community-oriented policing services, and the State Criminal Alien Assistance Program. These are programs that directly help our towns and communities. The CDBG Program grows local economies and improves the quality of life for families. It has assisted hundreds of millions of people with low and moderate incomes, stabilized neighborhoods, provided affordable housing, and improved the safety and quality of life of American citizens. The Cops on the Beat grant funds salaries and benefits for police officers who serve us every day by keeping our communities safe, and they deserve better than being dragged into partisan politics.

My colleague from Louisiana seeks to strip funding from localities that undertake the balancing of public safety considerations and refuse to act as Immigration and Customs Enforcement agents. But this bill goes even further than that. This bill isn't content with taking discretion away from local communities; it takes it away from the judicial branch. It adds new mandatory minimums when, as a nation, we are trying to move away from that approach. The new mandatory minimum sentences would have a crippling financial impact with no evidence that they would actually deter future violations of the law. They could cost American taxpayers hundreds of millions of dollars. I think that deserves a serious, thoughtful debate in the Judiciary Committee, with expert testimony on whether this really makes us safer or whether we are throwing away hard-earned taxpayer dollars. But we won't even get that debate because this bill was fast-tracked as a Republican priority, and it didn't even go through the regular committee process.

The U.S. Senate cannot nurture an environment that demonizes and dehumanizes Latinos and the entire immigrant community. By threatening to strip CDBG funding from cities, Senate Republicans are saying that it is OK to withhold funding from economically vulnerable American citizens, senior citizens, veterans, and children to promote their anti-immigrant agenda and that it is OK to cut COPS funding, which has long promoted public safety through community policing.

A one-size-fits-all approach that punishes State and local law enforcement agencies that engage in well-established community policing practices just doesn't make sense. Local communities and local law enforcement are better judges than Congress of what keeps their communities safe. Police need cooperation from the community to do their jobs. That is why over the past several years hundreds of localities across our Nation, with the support of some of the toughest police chiefs and sheriffs, have limited their involvement in Federal immigration enforcement out of concerns for community safety and violations of the Fourth Amendment. They need witnesses and victims to be able to come forward without fear of recrimination because of their immigrant status, and fear of deportation should never be a barrier to reporting crime or seeking help from the police. This fear undermines trust between law enforcement and the communities they protect and creates a chilling effect.

These policies were put in place because local jurisdictions don't want to do ICE's job for them. Effective policing cannot be achieved by forcing an unwanted role upon the police by threat of sanctions or withholding assistance, especially at a time when law enforcement agencies are strengthening police-community relations.

Furthermore, why do my Republican colleagues believe they know better than the local towns and citizens who live this day in and day out? They talk endlessly about decentralizing government, giving the power back to local communities, but not this time. It is no wonder that this bill is opposed by law enforcement, including the Fraternal Order of Police, the Law Enforcement Immigration Task Force, the U.S. Conference of Mayors, immigrant and Latino rights organizations, faith groups, and domestic violence groups, among others.

This bill is not a real solution to our broken immigration system. The bottom line is that we need comprehensive immigration reform. We passed bipartisan legislation in 2013, but we haven't had a real discussion in Congress for over 2 years.

A recent Pew poll found that 74 percent of Americans overall said that undocumented immigrants should be given a pathway to stay legally. That included 66 percent of Republicans, 74 percent of Independents, and 80 percent of Democrats who support a pathway to legal status for undocumented immigrants. This bipartisan support is not new.

Comprehensive immigration reform, previously passed in the Senate, brought millions of people out of the shadows who had to prove their identity, pass a criminal background check, pay taxes, and provide an earned path to citizenship so ICE could focus on the people who were true public safety threats. The bill also increased penalties for repeat border crossers. It included $46 billion in new resources, including no fewer than 38,000 trained, full-time, active Border Patrol agents deployed and stationed along the southern border. It increased the real GDP of our country by more than 3 percent in 2023 and 5.4 percent in 2033—an increase of roughly $700 billion in the first 10 years and $1.4 trillion in the second 10. It would have reduced the Federal deficit by $197 billion over the next decade and by another $700 billion in the following. That is almost $1 trillion in deficit spending reductions by giving 11 million people a pathway to citizenship. That was a real solution. That is the type of reform we need. That, in fact, is the opportunity that existed. Unfortunately, the other body, the House of Representatives, did not even have a vote. To the extent that Americans are less safe, it is because of their inaction that we are less safe today.

Tragedies should not be used to scapegoat immigrants. They should not be used to erode trust between law enforcement and our communities. We cannot let fear drive our policymaking.

So let's actively and collectively resist the demagoguery that threatens to shape American policymaking for the worse. I believe a vote to proceed is a vote against the Latino and immigrant communities of our country, and I hope that on a bipartisan basis we can reject it.

With that, I yield the floor.

Mrs. FEINSTEIN. Mr. President, I wish to discuss sanctuary cities.

Two women, Kate Steinle and Marilyn Pharis, were killed in California over the summer, both allegedly by undocumented individuals with criminal records.

The suspect in each case had recently been released from local custody without notice to Federal immigration officials, which could have resulted in those individuals being removed from the country instead of being released.

I believe these murders could have been prevented if there were open channels of communication between local law enforcement and Federal immigration authorities about dangerous individuals.

In both cases, those lines of communication broke down, and two women died.

In my view, local law enforcement agencies should be required to notify Federal authorities—if such notification is requested—that they plan to release a dangerous individual, such as a convicted felon.

This is a reasonable solution that would target those criminals who shouldn't be released back onto the street.

While I do support mandatory communication between local, State, and Federal officials, I do not support the bill before us today.

The bill we will soon be voting on would target all undocumented immigrants for deportation.

It would divert already stretched local law enforcement resources away from dangerous criminals and from policing in their own communities. I do not support such an action.

This bill also includes a detention requirement that goes beyond dangerous individuals—it would cover any immigrant sought to be detained.

This is a standard that could be abused in another administration, and it is potentially a huge unfunded mandate to impose on States and localities.

In addition to being an unfunded mandate, the bill would make drastic cuts to police departments, sheriffs departments, and local community programs.

Specifically it would cut the COPS Hiring Program; the State Criminal Alien Assistance Program, known as SCAAP; and the Community Development Block Grant Program.

Last year, 21 California jurisdictions received $13.2 million in COPS hiring grants to hire police officers.

California also received $57 million in SCAAP funds to help cover costs of holding undocumented immigrants.

And California communities received $356.9 million under the Community Development Block Grant Program.

As a former mayor, I know how important these funds are to local communities.

The bill would also impose lengthy Federal prison sentences on all undocumented immigrants.

This would include mothers crossing the border to see their children.

It would include agricultural workers who are vital to California's economy.

It would include other essentially innocent individuals who simply want to make a better life for themselves and their families.

In my view, this goes much too far, and I cannot support it.

I would, however, like to talk further about the murders of Kate Steinle and Marilyn Pharis and what I believe should be done to protect public safety.

Kate Steinle, a 32-year-old woman, was shot and killed in July while walking along San Francisco's Pier 14 with her father.

The suspected shooter, Juan Francisco Lopez-Sanchez, had a long criminal record.

He had seven felony convictions, including one for possession of heroin and another for manufacturing narcotics.

He had also been removed from the country five times.

The chain of events that led to Kate's murder began on March 23, when San Francisco County Sheriff Ross Mirkarimi requested that Lopez-Sanchez be transferred from Federal prison to San Francisco.

The sheriff's request was based on a 20-year-old marijuana possession warrant.

On March 26, Lopez-Sanchez was booked into San Francisco County jail.

However, the 20-year-old marijuana charge was quickly dropped, and Lopez-Sanchez was later released.

Immigration and Customs Enforcement had asked Sheriff Mirkarimi to let the agency know when Lopez-Sanchez would be released. That did not happen.

A simple phone call would have been enough, but Sheriff Mirkarimi failed to notify Federal officials.

In July, only a few months after his release, Lopez-Sanchez shot and killed Kate Steinle.

In fact, not only did the sheriff fail to notify, the failure was a consequence of a deliberate policy.

Just weeks before his office requested the transfer of Lopez-Sanchez, the sheriff adopted a policy forbidding his own deputies from notifying immigration officials.

The policy specifically states that sheriff department staff shall not provide release dates or times to immigration authorities.

Let me be clear: this isn't State law or even San Francisco law. This is the sheriff's own policy.

I believe this policy is wrong, and I have called on the sheriff to change it. San Francisco Mayor Ed Lee has made the same request.

On July 24, Marilyn Pharis was brutally attacked with a hammer and sexually assaulted in her home by two suspects.

The 64-year-old Air Force veteran died in the hospital from her injuries a week later.

One of the individuals charged with this heinous crime is a 20-year-old U.S. citizen named Jose Fernando Villagomez.

The other is a 29-year-old undocumented immigrant named Victor Aureliano Martinez Ramirez.

According to ICE, Martinez Ramirez was arrested in May 2014, but he had no prior felony convictions or deportations.

He was subject to what is called an ICE detainer request, asking the local jurisdiction to hold him until ICE could pick him up.

The local jurisdiction did not hold the suspect, nor did they notify ICE of his release.

In the ensuing months, Martinez Ramirez accumulated multiple misdemeanor convictions, including possession of methamphetamine and battery.

One of his convictions included a protection order requiring him to stay away from a particular individual.

On July 20, he pleaded guilty to additional misdemeanor charges of possessing a dagger and drug paraphernalia.

He was sentenced to 30 days, but that wasn't to begin until October 31. He was released from custody and, 4 days later, allegedly attacked, raped, and killed Marilyn Pharis in her own home.

I believe these two cases demonstrate the need for better communication between local, State, and Federal authorities before a dangerous individual with a criminal record is released.

When our committee was set to markup an earlier bill from Senator VITTER, I prepared a simple amendment to ensure such communication happens. That markup was cancelled.

I'd like to describe this approach now.

First, it would require notification by a State or local agency of the impending release of certain dangerous individuals, if ICE requests such notification.

It would apply to individuals where there is probable cause to believe they are aliens who are removable from the country and who pose a threat to the community.

Immigration offenses would be covered only if the individual had actually received more than 1 year in prison, which would happen for a person with a significant criminal history.

The amendment I prepared would not include harmful cuts to law enforcement and community programs, which I believe are unnecessary and unwise.

The legal precedents from the Supreme Court show that Congress can impose a reporting requirement on a State or local government, without threatening harmful funding cuts.

That is the approach I would take—I believe it would protect public safety without harming otherwise law-abiding immigrants or State or local law enforcement.

Before I conclude, I'd like to remind my colleagues that this is not a choice between being pro-immigrant or pro-criminal.

I am pro-immigrant. Immigrants make a tremendous contribution to this country and to my State.

They work some of the most difficult jobs, from agriculture to construction to hospitality.

They are part of the fabric of our country.

I, myself, am the daughter of an immigrant.

I strongly support comprehensive immigration reform, which I think is the only long-term solution to many of these problems.

I also support the President's executive actions to eliminate the threat of deportation for young people who have been raised here, as well as the parents of American citizens.

And I agree with immigrant advocates who want to prevent families from being separated because of a minor infraction like a broken taillight.

The position I support strikes a balance.

It would keep dangerous individuals off the street, while protecting otherwise law-abiding immigrants who are just here to work and provide their children with a better future.

I believe the deaths of Kate Steinle and Marilyn Pharis could have been prevented.

I believe we can and should fix the problems that led to their deaths by requiring that local officials notify Federal officials before they release dangerous criminals, if asked to do so.

I oppose Senator VITTER's bill, which would sweep up otherwise law-abiding immigrants and divert resources away from where they are most needed.

We should focus our efforts on dangerous criminals, and I hope that when we again take up comprehensive immigration reform, that is what happens.

I thank the Chair.

Mrs. BOXER. Mr. President, the death of Kate Steinle in San Francisco by a convicted felon who illegally crossed the border multiple times was horrific. It left a family heartbroken and shocked our community, our State, and our Nation.

We cannot allow a tragedy like this to happen again.

We should never give sanctuary to serious and violent felons, but this Republican bill is not the answer.

Getting rid of sanctuary cities will not reduce crime—in fact, it will only increase crime and make us less safe.

That is why this bill is opposed by law enforcement, immigrant rights organizations, faith groups, domestic violence groups, labor unions, housing and community development organizations, mayors of California's biggest cities, and the National League of Cities—as well as many others.

The truth is that sanctuary cities keep our neighborhoods safe by promoting trust and cooperation between police officers and immigrant communities. And that trust is essential to protecting all of us.

Let me give a quick example.

A few years ago in Seattle, more than two dozen Asian women were sexually assaulted in the same neighborhood over a 2-year period.

Because of the strong relationship between police and the community—a community where police are generally prohibited from asking about immigration status—many of the immigrant victims were willing to come forward and share information with the police, which led to the perpetrator's arrest.

Don't just take my word for it—listen to what law enforcement in our communities say about the importance of sanctuary city policies.

As former San Jose Police Chief Rob Davis said: ''We have been fortunate enough to solve some terrible cases because of the willingness of illegal immigrants to step forward, and if they saw us as part of the immigration services, I just don't know if they'd do that anymore.''

As Ohio Chief of Police Richard Biehl explained: ''Sanctuary policies and practices are not designed to harbor criminals. On the contrary, they exist to support community policing, ensuring that the community at large—including immigrant communities—trusts State and local law enforcement and feels secure in reporting criminal conduct.''

Ending sanctuary policies would keep the voices of immigrant victims and witnesses quiet.

That means crimes would go unreported, cases would go unsolved, and dangerous criminals would go unpunished.

Ending these policies would actually give sanctuary to dangerous criminals because, without the help of immigrant communities, these violent offenders will continue to threaten our safety.

We know this because there are many places in this country where immigrants do not feel safe coming forward.

As Texas Sheriff Lupe Valdez said: ''A lot of undocumented individuals came from areas where they can't trust the police. The uniform has pushed them into the shadows. Good law enforcement cannot be carried out this way.''

Just listen to some of the immigrants who were too terrified to come forward and report horrific crimes.

Take it from Maria, an immigrant survivor of serious domestic violence, who fled from Texas to Indiana, where her abuser tracked her down.

When he came to her house at midnight, she was too afraid to call 911—fearing she could be deported—so she called her lawyer over and over. Because it was the middle of the night, her attorney was not at work and came in the next morning to a series of frantic messages left on her voicemail.

Ultimately, Maria's abuser was not able to get into the house, but her life was in danger because she thought that law enforcement wasn't a safe option.

Take it from Cecilia, a young Guatemalan girl in Colorado.

Cecilia was sexually abused by a family friend at the age of 5. Her parents, undocumented immigrants, learned about the abuse, but they were terrified to report the crime to the police because they were told by family and friends that the police could not be trusted. They were told that, if they came forward, they would be reported to immigration and deported.

A year later, the same perpetrator sexually abused another young child. It wasn't until the father of that child contacted Cecilia's parents that they decided to go to the police together, and the perpetrator was caught and prosecuted.

But because of their initial fear of reporting the crime, another child was harmed.

So why would we pass a bill that could discourage victims or witnesses from coming forward for help?

Why would we pass a bill that would make it harder for law enforcement to solve crimes and keep our communities safe?

This Republican bill is also dangerous because it would cut off COPS grants that help communities protect residents by hiring officers.

We should be doing everything we can to help local police departments—not take away their ability to put officers on the street.

Republicans also want to punish communities by taking away their community development block grants, which would hurt thousands of working families who rely on these funds for safe, affordable housing and other critical services.

This GOP bill would also take away SCAAP funding, which reimburses State and local governments for the costs of incarcerating undocumented immigrants. This funding has been repeatedly slashed, and it has never been enough—especially in my State of California, which spends nearly $1 billion a year on these incarceration costs.

These cuts would have devastating impact on States and local communities.

Now, there are some California communities reviewing their specific policies and forging cooperation agreements with Federal immigration officials—and I think that's a good thing.

I believe that State and local officials should examine their policies to ensure that they are preserving the trust that law enforcement has built in our communities, while keeping serious and violent felons off our streets.

Unfortunately, this Republican bill would do the exact opposite—it would undermine the trust that has been developed between police and immigrant communities, and it would set back efforts to solve cases and put dangerous criminals behind bars.

The real question is: Why are we even considering this bill?

Why isn't Congress passing the bipartisan comprehensive immigration reform bill that the Senate passed more than 2 years ago?

That bipartisan bill would make our country safer by adding 20,000 more Border Patrol agents; increasing surveillance; and hiring additional prosecutors and judges to boost prosecutions of illegal border crossings.

The measure would also make clear that serious or violent felons will never get a pathway to citizenship or legal status.

And the bill would bring families out of the shadows—so that they don't fear being deported or separated from their families . . . so they feel comfortable cooperating with police and reporting crimes in their communities.

Let's make our communities safer by passing real immigration reform and by defeating this misguided Republican bill.

I urge my colleagues to vote no.

The PRESIDING OFFICER (Mr. CRUZ). The Senator from New York.

DONNELLY CONFIRMATION

Mr. SCHUMER. Mr. President, I am going to discuss the bill on the floor in a minute, but first I wish to take a moment to congratulate the newly confirmed district judge for the Eastern District of New York, Ann Donnelly. She just passed the Senate with a vote of 95 to 2—nearly unanimous and deservedly so.

There are few more qualified for a Federal judgeship than Ann Donnelly. She has dedicated her life to public service, having spent a quarter decade as a prosecutor in the prestigious New York County District Attorney's Office under Bob Morgenthau. She accumulated a host of awards there and rose through the leadership ranks of the office. Then, in 2009, she became a State court judge in New York, hearing a wide variety of cases. She has a stellar academic record, having graduated from the University of Michigan and Ohio State University School of Law.

I could tick off more of her accomplishments, and the list would be long, but Judge Donnelly is more than a brilliant resume. I know her well. She is at her core a kind, thoughtful, and compassionate person. Anyone who knows her or who has interacted with her even briefly knows she is fair, open-minded, and has exactly the kind of temperament that will make her an exceptional Federal judge.

I congratulate Ann Donnelly and her family—particularly her mother—on her confirmation. I know her mother is so proud of her. It is a milestone day in her career and a bright day for the Eastern District of New York.

Mr. President, today the Senate will turn its attention to a divisive immigration bill that has no hope of becoming law. Today's vote won't be on a comprehensive bill, as was the one the Senate passed 2 years ago—one that secures our borders, provides a jolt to the economy, provides a pathway to citizenship for hard-working, law-abiding immigrants who pay their taxes to get right with the law.

I want to be clear with the American people on this. Today's vote is nothing but a political show vote. Senator VITTER knows his bill has no chance of passing the Senate or being signed into law. As stated by my friend the Republican junior Senator from Nevada—here is what he said: ''You know we have votes because people are running for president, so I am not surprised we have votes because people are running for governor.'' No other sentence sums it up better as to what a waste of time this is, and that is to say nothing about the substance of the bill, which has drawn opposition from nearly every important interest group. A broad coalition of major law enforcement groups, faith groups, labor, cities, elected officials, housing advocates, and immigrant rights groups oppose this bill. I suspect there are Members of the Republican caucus who oppose many parts of it. Why? Because it is a bill that would jeopardize hundreds of millions of dollars in the name of punishing immigrants and cities where they live.

This bill would strip away community development block grants, community COPS grants to hire more cops, and SCAAP, a proposal that funds jurisdictions that are doing what many on the other side want them to do by locking up unauthorized immigrants who commit crimes. Everyone believes that if a person commits a serious crime unrelated to being an immigrant—not like crossing the border or forging a document but a serious crime—law enforcement should be required to cooperate and those folks should be deported, plain and simple. But in the name of trying to help law enforcement, this bill hurts law enforcement because it will take away so many of the grants law enforcement needs. It will take away the grants that help create a way of incarcerating those who commit serious crimes.

All of these cuts would come while also astronomically increasing the size of prison population and related costs, without decreasing the deficit by a single dime. This will put a huge burden on our State and local taxpayers. Their taxes would go way up if this bill were passed into law and implemented.

To be clear, the death of Kathryn Steinle in San Francisco was tragic. It never should have happened. I mourn not only her family but the family of any American killed in a senseless act of gun violence. For people like the killer of Ms. Steinle, law enforcement should cooperate with the Federal authorities and deport those folks.

This is not the way to exercise better law enforcement. Punishing cities and communities and yanking Federal funding from cops will not get us to a better immigration system or safeguard our communities.

The bill we passed in 2013, which I was proud to author with a number of Democratic and Republican colleagues, is the opposite of this bill in every way. Our bill was supported by a broad coalition of groups, from business, labor, faith communities, immigrant communities, and law enforcement. Our bill paid for itself and went on to decrease the deficit by $160 billion over 10 years and to increase GDP by 3.3 percent. Our bill secured the border—this bill doesn't do that—not only with more resources and staff but by cracking down on repeat border crossers and those who overstay their visas. It did it in a smart way. The goal of our friend from Louisiana isn't accomplished in his bill, but it is in comprehensive immigration reform—the goal of making sure those who are repeat border crossers and those who overstay their visas are dealt with properly.

Our bill paved a tough but fair pathway to citizenship, shielding law-abiding immigrants from deportation, fostering trust with law enforcement, and exposing the criminals in their communities who would rather live in the shadows.

Our bill was a bipartisan compromise. There is no compromise here. I daresay many of my colleagues on the other side of the aisle, when they look at provisions in this bill, do not like them. This is a show vote—a vote, as my Republican colleague from Nevada said, to help someone in his quest for political office.

There are so many vitally important policy debates we could be turning to today. Instead, the Senate Republican leadership insists on leading us into this dark, divisive place for nothing more than political theater. Think of the urgent bipartisan issues we should be working on, including the debt ceiling. We are about to default because of the shenanigans going on on the other side. The Perkins Loan Program so that kids can go to college; the land and water conservation programs are expiring. The highway bill—we don't have a highway bill, yet we are doing this. And if we don't take action by the end of the year, millions of seniors will see a 52-percent increase in their Medicare bill. How many Americans would want us to do that and not the divisive show vote that has no chance of passing?

I urge my colleagues to oppose this bill. Just as importantly, I beg my colleagues to join us on this side of the aisle in turning to a serious debate on comprehensive immigration reform—something they have so far refused to do.

Thank you, Mr. President.

I yield the floor.

The PRESIDING OFFICER. The Senator from Pennsylvania.

The Senator is advised that the Senate is under an order to recess at this time.

Mr. TOOMEY. Mr. President, I ask unanimous consent that I be recognized for such time as I may consume and that Senator HIRONO be recognized following my remarks.

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

Mr. TOOMEY. Mr. President, I rise to speak on S. 2146, the Stop Sanctuary Policies and Protect Americans Act, which the Senate will vote on shortly and which our colleagues have been speaking about.

First, I want to recognize and thank my colleagues for joining in this effort—Senator VITTER, Senator GRASSLEY, Senator CRUZ, and Senator JOHNSON—and introducing this very important bill. I can't believe the way it is being mischaracterized, and I will try to address some of those mischaracterizations.

Let's be clear. This bill is about keeping our communities safe from violent crime. That is what it is about. It is necessary because of the sanctuary cities that we have across America.

This is not a manufactured problem. This is a very real problem. There is one father who knows about it all too well. Jim Steinle was walking arm in arm with his daughter on a pier in San Francisco. Suddenly a gunman leaps out, opens fire, and hits Kate. She falls into her father's arms and pleads, ''Help me, dad,'' while she bleeds to death.

What is so outrageous about this, among other things, is that the shooter never should have been on the pier that day, in the first place. He was an illegal immigrant who had been convicted of seven felonies. He had been deported

five times, and there he is on the San Francisco pier, shooting and killing an innocent woman. It is more outrageous than that. Just 3 months earlier, the Department of Homeland Security had asked the San Francisco Police Department, when they had picked up this man, to hold him until DHS officials could come and get him. They had made that specific request when this man was in the custody of the San Francisco Police Department, but San Francisco refused to cooperate. Knowing that DHS wanted them to hold this man for a short period of time until their agents could get there and take him into custody, having had that request from DHS, San Francisco said no, and they released him so he could then go out and commit a murder.

Why in the world would they release a man such as this when DHS has asked them to hold him? It is because San Francisco is a sanctuary city. What that means is that it is the policy of the city of San Francisco—having commanded their local law enforcement, their police department—to not cooperate with Federal officials seeking to prosecute immigration issues. Even when they want to cooperate, they are forbidden from cooperating. Think about how absurd this is.

If Federal officials had called the San Francisco Police Department about any other kind of crime—larceny, burglary, a trademark violation—they would have been happy to cooperate. They would have cooperated, in fact. But because the crime was related to illegal immigration, the San Francisco Police Department's hands were tied. The police were forced to release the man who would then go on and kill Kate Steinle. As a father of three young children, I can't even begin to think about the pain that the Steinles just went through, and what is so maddening is that it was entirely unnecessary.

Sadly, this is not the only case, as you know. According to the Department of Homeland Security, during an 8-month period last year, sanctuary jurisdictions—cities and counties that have adopted this policy of noncooperation—have released over 8,000 illegal immigrants they had in their custody, and 1,800 of these were later arrested for criminal acts. This includes two cities that refused to hold individuals who had been arrested for child sexual abuse. In both cases the individuals were later arrested for sexually assaulting young children. This is how outrageous this has become.

For the record, let me make it clear that I completely understand that the vast majority of immigrants would not commit these crimes. That is not what this is about. But the truth of the matter is that any large group of individuals is going to have a certain number of criminals within it. Of the 11 million people who are here illegally, some are inevitably violent criminals.

The Stop Sanctuary Policies and Protect Americans Act provides a solution to this in three parts. First, under our legislation sanctuary jurisdictions will lose certain Federal funds. If a city or county or municipality decides they will declare or forbid their law enforcement officials from cooperating and even sharing information with Federal Department of Homeland Security officials, they will lose some Federal funding.

Second, this legislation includes Kate's Law. This provides for a mandatory minimum 5-year sentence for a person who reenters the United States illegally after having been convicted of an aggravated felony or having been convicted twice before of illegal reentry.

Finally, there is the third part of this legislation. Across America dozens of municipalities that had been cooperating with Federal immigration officials have been forced to become sanctuary communities or counties because several Federal courts have held that local law enforcement may not cooperate when DHS asks them to hold an illegal immigrant. They maintain that there is not the statutory authority for local law enforcement to do so. Therefore, if the local police were to cooperate, as they should, they would be liable for damages, and this would apply even to dangerous criminal cases. We solve that problem by making it clear that when local law enforcement is acting in a fashion consistent with what DHS is requesting—what DHS has the authority to do themselves—then there would be no such legal liability.

Some of my Democratic colleagues have said that we don't need this legislation and that all we need is greater cooperation between Federal and local law enforcement. Well, that is absolutely factually incorrect. It is not possible to have the level of cooperation that we need to have because of these court decisions, because the court decisions effectively are precluding the kind of cooperation that we need. That is why Congress needs to act.

We need to make it clear that local law enforcement can in fact hold somebody that the Department of Homeland Security needs to have held, just as the Department of Homeland Security has that authority themselves. The Stop Sanctuary Policies and Protect Americans Act provides a valid solution. It confirms that local law enforcement officers are allowed to cooperate when Federal officials ask them to hold illegal immigrants.

It is carefully drafted to protect individual liberties. If an individual's civil liberties or constitutional rights are violated, than that individual can still file suit and can still seek a remedy, and that is as it should be. But this legislation to stop sanctuary policies act really should have very broad bipartisan support.

Let's keep in mind the people we are talking about here. As a practical matter, the only cases in which this applies is that small subset of illegal immigrants who even the Obama administration wishes to hold for deportation—only that small subset of people that the Obama administration believes is dangerous enough to warrant removal. Really, we can't even have local law enforcement officials cooperate under those circumstances?

President Obama's own Secretary of Homeland Security has declared that sanctuary cities are ''not acceptable.'' He has described them as ''counterproductive to public safety.'' There is no real basis for voting no on this.

Opponents have turned to misrepresenting this in many ways, but the facts are overwhelming.

There are three national law enforcement groups that have written a powerful letter addressing some of the misrepresentations that have been made about this bill. They have reaffirmed their support for this bill. They include the National Sheriffs' Association, the National Association of Police Organizations, and the Federal Law Enforcement Officers Association.

Mr. President, I ask unanimous consent to have their letter printed in the RECORD.

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

OCTOBER 20, 2015.

Senator DAVID VITTER,
U.S. Senate, Hart Senate Office Bldg., Washington, DC.
Chairman CHUCK GRASSLEY,
U.S. Senate, Hart Senate Office Bldg., Washington, DC.
Senator RON JOHNSON,
U.S. Senate, Hart Senate Office Bldg., Washington, DC.
Senator PAT TOOMEY,
U.S. Senate, Russell Senate Office Bldg., Washington, DC.
Senator TED CRUZ,
U.S. Senate, Russell Senate Office Bldg., Washington, DC.

DEAR SENATORS VITTER, TOOMEY, GRASSLEY, CRUZ, AND JOHNSON: On behalf of the National Sheriffs' Association, the National Association of Police Organizations, and the Federal Law Enforcement Officers Association and the local, state, and federal law enforcement officers we represent, we write to reiterate out support for the Stop Sanctuary Policies and Protect Americans Act (S.2146) and to correct some misrepresentations regarding the Act.

As the law enforcement officers on the front lines working to protect our communities, we know firsthand the challenges facing police officers. We know when a bill makes our jobs more difficult and when a bill makes our jobs easier.

We have been surprised to hear some misrepresent this bill and its effects on law enforcement.

For example, some have claimed that the Stop Sanctuary Policies Act will ''requir[e] state and local law enforcement to carry out the federal government's immigration enforcement responsibilities,'' and thus ''the federal government would be substituting its judgment for the judgment of state and local law enforcement agencies.'' Nothing in the Stop Sanctuary Policies Act requires local law enforcement ''to carry out federal immigration responsibilities.'' Removing illegal immigrants remains the exclusive province of the federal government. The bill simply withholds certain federal funds from jurisdictions that prohibit their local law enforcement officers from cooperating with

federal officials in the limited circumstance of honoring an immigration detainer. It is politicians in sanctuary jurisdictions who, by tying the hands of local law enforcement, are ''substituting [their] judgment for the judgment of state and local law enforcement.''

Others have resorted to scare tactics, warning that that S.2146 will lead to the deportation of those who report crimes to law enforcement. This is simply false. The bill provides that if a jurisdiction has a policy that it will not inquire about the immigration status of crime victims or witnesses, the jurisdiction will not be deemed a sanctuary jurisdiction and will not lose any federal funds.

To be clear: We believe the Stop Sanctuary Policies Act will make America safer, enhance the ability of police to protect and serve, and provide greater flexibility for law enforcement officers at every level—federal, state, and local.

We also write to address those Members of Congress who insist that the Stop Sanctuary Policies Act is not needed; instead, Congress should ''encourage'' local officers to cooperate with federal officials. This ignores one crucial fact: Across America, federal courts have issued decisions forbidding local officers from cooperating with federal requests to hold an illegal immigrant. These decisions provide that local law enforcement and municipalities may be sued if they cooperate with federal officials to detain dangerous criminals. Under these decisions, even if a federal official would have had the authority to hold the individual, local law enforcement can still be sued.

Too often, local law enforcement officers are left with a terrible choice: Either release an individual who has been convicted of or arrested for violent crimes, or be sued and lose funds that are needed to protect our communities. As a result of these lawsuits, scores of cities and counties across America have become sanctuary jurisdictions.

The Stop Sanctuary Policies Act provides a solution. The bill confirms that local law enforcement may cooperate with federal requests to hold an illegal immigrant. The bill provides that when local officers comply with such requests, they are delegated the same powers to hold an illegal immigrant as a DHS official would have. If the detention would have been legal if carried out by the Department of Homeland Security (DHS), then under S.2146 it is still legal; it does not become a crime simply because it is a local sheriff acting instead of a DHS official.

This provision was carefully drafted to protect individual liberties. It preserves an individual's ability to sue for a violation of a constitutional or civil rights, regardless of whether the violation was the result of negligence or was purposeful. Under S.2146, if there was no basis to detain the individual—DHS issued the request for someone in the U.S. legally—the individual may still sue for a violation of rights. The difference is that the party responsible for the error, the federal government, is liable; not a local police officer or jailer acting in good faith. If a local law enforcement officer acts improperly—mistreating an individual or continuing to hold an individual after federal officials issue a release order—the individual may sue, with the local officer liable for all costs and judgments.

Contrary to the assertions of the American Civil Liberties Union (ACLU)—the party that has orchestrated these lawsuits against local law enforcement officers—the Stop Sanctuary Policies Act is fully consistent with the Fourth Amendment. In a letter to Congress, the ACLU states, ''The Fourth Amendment provides that the government cannot hold anyone in jail without getting a warrant or the approval of a judge.'' The fact is that the Constitution requires probable cause to detain an individual, which can be established by a judicial warrant issued before the arrest or by a demonstration of probable cause after the arrest. Otherwise police could never arrest someone whom they see committing a crime. The Stop Sanctuary Policies Act does not alter the requirement for probable cause. To the contrary, S.2146 explicitly preserves an individual's ability to sue if he or she is held without probable cause or has suffered any other violation of a constitutional right.

The ACLU also tries scare tactics. It claims that the Stop Sanctuary Policies Act includes ''provisions requiring DHS to absorb all liability in lawsuits brought by individuals unlawfully detained in violation of the Fourth Amendment.'' This is false. If a lawsuit alleges that a local officer knowingly violated Fourth Amendment or other constitutional rights, then under S.2146, the individual officer will bear all liability—not the federal government. For some lawsuits, the U.S. will be substituted as defendant—specifically, suits alleging that that the immigration detainer should not have been issued. But such a claim could already be brought against the U.S. under existing law; thus, S.2146 does not create a new source of liability for the federal government. S.2146 simply provides that if the federal government made the error, the federal government should be the defendant.

We, the law enforcement officers of America, are on the front lines day after day. We know the challenges of apprehending criminals and the difficulties of working with crime victims and witnesses—especially those who may be fearful of local and federal authorities. Based on our collective knowledge and experience, we strongly support the Stop Sanctuary Policies Act (S.2146) and urge the Senate to pass this important legislation.

Sincerely,

NATIONAL SHERIFFS' ASSOCIATION.
NATIONAL ASSOCIATION OF POLICE ORGANIZATIONS.
FEDERAL LAW ENFORCEMENT OFFICERS ASSOCIATION.

Mr. TOOMEY. Mr. President, let me finish by reminding my colleagues that the vote we are about to have is not actually a vote on this bill in its current form. If Members object to a provision in it or they want to add a provision in it, then, by all means, let's vote to get on the bill. Let's open up debate, and we will have amendments, we will have a discussion, and we will have a debate. They are free to attempt to improve this bill and modify this bill, as they see fit.

This vote today is not a final passage vote. It is a vote on whether the issue of sanctuary jurisdictions is important enough to merit the Senate's consideration.

I was just shocked to hear one of our colleagues describe this bill as a waste of time. Really, a waste of time? That is unbelievable. How could the lives of Kate Steinle and the other victims who have been lost because of this ridiculous policy be a waste of the Senate's time when the courts are precluding the cooperation between local and Federal law enforcement officials because we have not acted? There is a simple solution. It starts with passing a motion to proceed so we can get on this bill and hopefully complete it successfully. I think the lives of Kate Steinle and the other victims are not a waste of time. I think we should be addressing this issue. We should be addressing it today.

I urge my colleagues to vote aye so that we can begin considering this very important—and it should be broadly supported—bipartisan piece of legislation.

I yield the floor.

The PRESIDING OFFICER. The Senator from Hawaii.

Ms. HIRONO. Mr. President, I would like to urge my colleagues to oppose S. 2146, the Stop Sanctuary Policies and Protect Americans Act.

Hundreds of cities and local jurisdictions across our country have financial, constitutional, and public safety concerns with using scarce local tax dollars to hold immigrants in jail when they otherwise would be entitled to release under the law. These cities and towns are being called sanctuary cities because they have made a local and fact-based choice to keep their communities safe rather than serve as an arm of immigration enforcement.

This bill would create new criminal penalties for undocumented immigrants and make life even harder for them, most of whom are honest, hard-working people, not criminals. The bill also takes severe steps to penalize these sanctuary cities by stripping them of critical community block grants and Federal homeland security and law enforcement funding. While this bill purports to protect our communities, it is strongly opposed by law enforcement, victims' advocates, and local and State government leaders.

Why do they oppose this bill?

Demonizing our immigrant communities and using them as scapegoats does not make America safer. Decades of research shows the following: that immigrants as a group are not a threat to public safety, that immigrants are less likely to commit serious crimes than the rest of Americans, and that the higher rates of immigration are associated with lower rates of violent crime.

Law enforcement is clear. This bill would limit their ability to keep all people in their communities safe. Good community policy requires collaboration and trust. Our law enforcement officials want to spend their time going after people who truly pose a threat to our safety. This bill would have us spend limited resources pursuing hard-working though undocumented members of their communities with no criminal history. Community law enforcement should not be coerced, because that is what this bill would require. It is a requirement. Community law enforcement should not be coerced into serving as an arm of Federal Immigration and Customs Enforcement. That is what this bill does. Nobody is talking about voluntary collaboration and support for Federal Government

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.

The PRESIDING OFFICER. The Senator from North Carolina.

AMENDMENT NO. 2716

(Purpose: In the nature of a substitute)

Mr. BURR. Mr. President, as under the previous order, I call up the Burr-Feinstein amendment, which is at the desk, and I ask unanimous consent that it be reported by number.

The PRESIDING OFFICER. Without objection, the clerk will report the amendment by number.

The senior assistant legislative clerk read as follows:

The Senator from North Carolina [Mr. BURR] proposes an amendment numbered 2716.

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

Mr. BURR. Mr. President, for the information of all Senators, this substitute includes agreed-upon language on the following amendments: Carper, No. 2615; Carper, No. 2627; Coats, No. 2604; Flake, No. 2580; Gardner, No. 2631; Kirk, No. 2603; Tester, No. 2632; Wyden, No. 2622, and, I might add, a handful of amendments that have been worked out in addition to those which were part of that unanimous consent agreement by both the vice chair and myself.

The vice chair and I have a number of amendments to be made pending under the previous consent order, and I ask unanimous consent that they be called up and reported by number.

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

AMENDMENT NO. 2581, AS MODIFIED, TO AMENDMENT NO. 2716

Mr. BURR. Mr. President, I call up the Cotton amendment No. 2581, as modified, to correct the instruction line.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from North Carolina [Mr. BURR], for Mr. COTTON, proposes an amendment numbered 2581, as modified, to amendment No. 2716.

The amendment is as follows:

(Purpose: 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)

On page 31, strike line 13 and insert the following:

authority regarding a cybersecurity threat; and

(iii) communications between a private entity and the Federal Bureau of Investigation or the United States Secret Service regarding a cybersecurity threat;

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Mr. President, let me add at this time that the vice chairman and I have worked aggressively, as have our staffs, to incorporate the suggestions and the concerns Members and companies have raised with us. If we believed they made the legislation stronger—stronger from the standpoint of minimizing data loss and stronger from the standpoint of the privacy concerns—let me assure my colleagues we have accepted those and we have incorporated them in the managers' amendment. If, in fact, we couldn't agree or felt that it in any way was detrimental to the legislation, the vice chair and I have agreed to oppose those amendments.

I think it is important that this bill represent exactly what we have sold: an information sharing bill, a bill that is voluntary.

So I would suggest to those who hear this debate and say ''I don't really understand all this cyber stuff. I hear about it and don't really understand it,'' let me put it in these terms. What this legislation does is it creates a community watch program, and like any neighborhood watch program, the spirit of what we are trying to do is to protect the neighborhood. It doesn't mean that every resident on every street in that community in that neighborhood is going to be a participant, but it means that neighborhood is committed to making sure that if crimes are happening, they are out there to stop them, to report them, and maybe through reporting them, the number of crimes over time will continue to decrease.

Well, I would share with you that is what we are doing with the cyber security bill. We are out now trying to set up the framework for a community watch program, one that is voluntary, that doesn't require every person to participate, but it says: For those of you who can embrace this and can report the crimes, it is not only beneficial to you, it is beneficial to everybody.

So I respect the fact there are a few companies out there saying: This is no good; we shouldn't have this. Really? Do you want to deny this to everybody? There are a heck of a lot of businesses that have made the determination that this is beneficial to their business, that it is beneficial to their sector.

This is beneficial to the overall U.S. economy. That is what the Senate is here to do. We are not here to pick winners and losers; we are here to create a framework everybody can operate in that advances the United States in the right direction.

Shortly we will have an opportunity to make pending some additional amendments, and I encourage all Members, if your amendment is pending, to come down and debate it. If you have additional amendments, please come down and offer them and debate them. With the cooperation of Members, we can process these in a matter of days and we can then send this out of the Senate and be at a point where we could conference with the House.

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

The PRESIDING OFFICER (Ms. AYOTTE). Without objection, it is so ordered.

AMENDMENT NO. 2552, AS MODIFIED, TO AMENDMENT NO. 2716

Mrs. FEINSTEIN. Madam President, I call up the Coons amendment No. 2552, as modified.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from California [Mrs. FEINSTEIN], for Mr. COONS, proposes an amendment numbered 2552, as modified, to amendment No. 2716.

The amendment, as modified, is as follows:

(Purpose: To modify section 5 to require DHS to review all cyber threat indicators and countermeasures in order to remove certain personal information)

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 4 that are received through the process described in subsection (c) of this section and that satisfy the requirements of the guidelines developed under subsection (b)—

(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 4 in a manner other than the 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 Act, 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 Act, including the extent, if any, to which such cyber threat indicators may be used by the Federal Government; and

(D) ensure there is—

(i) an audit capability; and

(ii) appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this Act 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 shall develop and make publicly available guidance to assist entities and promote sharing of cyber threat indicators with Federal entities under this Act.

(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 Act that would be unlikely to include personal information of or identifying a specific person not necessary to describe or identify a cyber security threat.

(ii) Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be necessary to describe or identify a cybersecurity threat.

(iii) Such other matters as the Attorney General considers appropriate for entities sharing cyber threat indicators with Federal entities under this Act.

(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 Act.

(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 Act.

(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 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 impact on privacy and civil liberties of activities by the Federal Government under this Act;

(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of or identifying 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 Act; 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 of or identifying 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 of or identifying 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 Act; 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 Act 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) communications between a Federal entity and a private entity regarding a previously shared 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 review all cyber threat indicators and defensive measures received and remove any personal information of or identifying a specific person not necessary to identify or describe the cybersecurity threat before sharing such 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 Act; 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.

The PRESIDING OFFICER. The Senator from North Carolina.

AMENDMENT NO. 2582 TO AMENDMENT NO. 2716

Mr. BURR. Madam President, I call up the Flake amendment No. 2582.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from North Carolina [Mr. BURR], for Mr. FLAKE, proposes an amendment numbered 2582 to amendment No. 2716.

The amendment is as follows:

(Purpose: To terminate the provisions of the Act after six years)

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 6-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 Senator from California.

AMENDMENT NO. 2612, AS MODIFIED, TO AMENDMENT NO. 2716

Mrs. FEINSTEIN. Madam President, I call up the Franken amendment No. 2612, as modified.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from California [Mrs. FEINSTEIN], for Mr. FRANKEN, proposes an amendment numbered 2612, as modified, to amendment No. 2716.

The amendment, as modified, is as follows:

(Purpose: To improve the definitions of cybersecurity threat and cyber threat indicator)

Beginning on page 4, strike line 12 and all that follows through page 5, line 21, and insert the following:

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

(B) EXCLUSION.—The term ''cybersecurity threat'' does not include any action that

solely involves a violation of a consumer term of service or a consumer licensing agreement.

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

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

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

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

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

(E) malicious cyber command and control;

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

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

The PRESIDING OFFICER. The Senator from North Carolina.

AMENDMENT NO. 2548, AS MODIFIED, TO AMENDMENT NO. 2716

Mr. BURR. Madam President, I call up the Heller amendment No. 2548, as modified, to correct the instruction line.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from North Carolina [Mr. BURR], for Mr. HELLER, proposes an amendment numbered 2548, as modified, to amendment No. 2716.

The amendment, as modified, is as follows:

(Purpose: To protect information that is reasonably believed to be personal information or information that identifies a specific person)

On page 12, line 19, strike ''knows'' and insert ''reasonably believes''.

The PRESIDING OFFICER. The Senator from California.

AMENDMENT NO. 2587, AS MODIFIED, TO AMENDMENT NO. 2716

Mrs. FEINSTEIN. Madam President, I call up the Leahy amendment No. 2587, as modified.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from California [Mrs. FEINSTEIN], for Mr. LEAHY, proposes an amendment numbered 2587, as modified, to amendment No. 2716.

The amendment, as modified, is as follows:

(Purpose: To strike the FOIA exemption)

Beginning on page 35, strike line 1 and all that follows through page 35, line 13.

The PRESIDING OFFICER. The Senator from North Carolina.

AMENDMENT NO. 2564, AS MODIFIED, TO AMENDMENT NO. 2716

Mr. BURR. Madam President, I call up the Paul amendment No. 2564, as modified, to correct the instruction line.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from North Carolina [Mr. BURR], for Mr. PAUL, proposes an amendment numbered 2564, as modified, to amendment No. 2716.

The amendment, as modified, is as follows:

(Purpose: To prohibit liability immunity to applying to private entities that break user or privacy agreements with customers)

On page 40, after line 24, insert the following:

(d) EXCEPTION.—This section shall not apply to any private entity that, in the course of monitoring information under section 4(a) or sharing information under section 4(c), breaks a user agreement or privacy agreement with a customer of the private entity.

The PRESIDING OFFICER. The Senator from California.

AMENDMENT NO. 2557 TO AMENDMENT NO. 2716

Mrs. FEINSTEIN. Madam President, I call up the Mikulski amendment No. 2557.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from California [Mrs. FEINSTEIN], for Ms. MIKULSKI, proposes an amendment numbered 2557 to amendment No. 2716.

The amendment is as follows:

(Purpose: To provide amounts necessary for accelerated cybersecurity in response to data breaches)

At the appropriate place, insert the following:

SEC. _____. FUNDING.

(a) IN GENERAL.—Effective on the date of enactment of this Act, there is appropriated, out of any money in the Treasury not otherwise appropriated, for the fiscal year ending September 30, 2015, an additional amount for the appropriations account appropriated under the heading ''SALARIES AND EXPENSES'' under the heading ''OFFICE OF PERSONNEL MANAGEMENT'', $37,000,000, to remain available until September 30, 2017, for accelerated cybersecurity in response to data breaches.

(b) EMERGENCY DESIGNATION.—The amount appropriated under subsection (a) is designated by the Congress as an emergency requirement pursuant to section 251(b)(2)(A)(i) of the Balanced Budget and Emergency Deficit Control Act of 1985, and shall be available only if the President subsequently so designates such amount and transmits such designation to the Congress.

AMENDMENT NO. 2626 TO AMENDMENT NO. 2716

Mrs. FEINSTEIN. Madam President, I call up the Whitehouse amendment No. 2626.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from California [Mrs. FEINSTEIN], for Mr. WHITEHOUSE, proposes an amendment numbered 2626 to amendment No. 2716.

The amendment is as follows:

(Purpose: To amend title 18, United States Code, to protect Americans from cybercrime)

At the end, add the following:

SEC. ____. STOPPING THE SALE OF AMERICANS' FINANCIAL INFORMATION.

Section 1029(h) of title 18, United States Code, is amended by striking ''if—'' and all that follows through ''therefrom.'' and inserting ''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. ____. SHUTTING DOWN BOTNETS.

(a) AMENDMENT.—Section 1345 of title 18, United States Code, is amended—

(1) in the heading, by inserting ''**and abuse**'' after ''**fraud**'';

(2) in subsection (a)—

(A) in paragraph (1)—

(i) in subparagraph (B), by striking ''or'' at the end;

(ii) in subparagraph (C), by inserting ''or'' after the semicolon; and

(iii) by inserting after subparagraph (C) the following:

''(D) violating or about to violate paragraph (1), (4), (5), or (7) of section 1030(a) where such conduct would affect 100 or more protected computers (as defined in section 1030) during any 1-year period, including by denying access to or operation of the computers, installing malicious software on the computers, or using the computers without authorization;''; and

(B) in paragraph (2), by inserting '', a violation described in subsection (a)(1)(D),'' before ''or a Federal''; and

(3) by adding at the end the following:

''(c) A restraining order, prohibition, or other action described in subsection (b), if issued in circumstances described in subsection (a)(1)(D), may, upon application of the Attorney General—

''(1) specify that no cause of action shall lie in any court against a person for complying with the restraining order, prohibition, or other action; and

''(2) provide that the United States shall pay to such person a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in complying with the restraining order, prohibition, or other action.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of section for chapter 63 is amended by striking the item relating to section 1345 and inserting the following:

''1345. Injunctions against fraud and abuse.''.

SEC. ____. AGGRAVATED DAMAGE TO A CRITICAL INFRASTRUCTURE COMPUTER.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer, if such damage results in (or, in the case of an attempted offense, would, if completed have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with such computer.

''(b) PENALTY.—Any person who violates subsection (a) shall, in addition to the term of punishment provided for the felony violation of section 1030, be fined under this title, imprisoned for not more than 20 years, or both.

''(c) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place any person convicted of a violation of this section on probation;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for the felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such violation to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, if such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.

''(d) DEFINITIONS.—In this section

''(1) the terms 'computer' and 'damage' have the meanings given the terms in section 1030; and

''(2) the term 'critical infrastructure' has the meaning given the term in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)).''.

(b) TABLE OF SECTIONS.—The table of sections for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. ___. STOPPING TRAFFICKING IN BOTNETS.

(a) IN GENERAL.—Section 1030 of title 18, United States Code, is amended—

(1) in subsection (a), by striking paragraph (6) and inserting the following:

''(6) knowing such conduct to be wrongful, intentionally traffics in any password or similar information, or any other means of access, further knowing or having reason to know that a protected computer would be accessed or damaged without authorization in a manner prohibited by this section as the result of such trafficking;'';

(2) in subsection (c)—

(A) in paragraph (2), by striking '', (a)(3), or (a)(6)'' each place it appears and inserting ''or (a)(3)''; and

(B) in paragraph (4)—

(i) in subparagraph (C)(i), by striking ''or an attempt to commit an offense''; and

(ii) in subparagraph (D), by striking clause (ii) and inserting the following:

''(ii) an offense, or an attempt to commit an offense, under subsection (a)(6);''; and

(3) in subsection (g), in the first sentence, by inserting '', except for a violation of subsection (a)(6),'' after ''of this section''.

AMENDMENT NO. 2621, AS MODIFIED, TO AMENDMENT NO. 2716

Mrs. FEINSTEIN. Madam President, I call up the Wyden amendment No. 2621, as modified.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from California [Mrs. FEINSTEIN], for Mr. WYDEN, proposes an amendment numbered 2621, as modified, to amendment No. 2716.

The amendment, as modified, is as follows:

(Purpose: To improve the requirements relating to removal of personal information from cyber threat indicators before sharing)

On page 17, strike lines 9 through 22 and insert the following:

(A) review such cyber threat indicator and remove, to the extent feasible, any personal information of or identifying a specific individual that is not necessary to describe or identity a cybersecurity threat; or

(B) implement and utilize a technical capability configured to remove, to the extent feasible, any personal information of or identifying a specific individual contained within such indicator that is not necessary to describe or identify a cybersecurity threat.

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Madam President, as the vice chair and I have said numerous times this afternoon, nothing would make us happier than for Members to come to the floor. We have amendments pending. We have a managers' amendment. Everybody knows exactly what is in this bill. Let's start the debate. Let's vote on amendments. Let's end this process in a matter of days. We are prepared to vote on every amendment.

So at this time, I ask unanimous consent that on Thursday, October 22, at 11 a.m., the Senate vote on the pending amendments to the Burr-Feinstein substitute to S. 754, with a 60-vote threshold for those amendments that are not germane; and that following the disposition of the amendments, the substitute, as amended, if amended, be agreed to, the bill, as amended, be read a third time, and the Senate vote on passage with a 60-vote threshold for passage.

The PRESIDING OFFICER. Is there objection?

Mr. WYDEN. Reserving the right to object.

The PRESIDING OFFICER. The Senator from Oregon.

Mr. WYDEN. Madam President, I certainly support most of the amendments that were just described. However, I am especially troubled about amendment No. 2626, which would significantly expand a badly outdated Computer Fraud and Abuse Act. I have sought to modernize the Computer Fraud and Abuse Act, and I believe that amendment No. 2626 would take that law—the Computer Fraud and Abuse Act—in the wrong direction. I would object to any unanimous consent request that includes that amendment. Therefore, I object to this request.

The PRESIDING OFFICER. Objection is heard.

The Senator from North Carolina.

Mr. BURR. Madam President, the Senate functions best when Members are free to come to the floor and offer amendments, debate the amendments, and have a vote on the amendments. I might even share Senator WYDEN's concerns about that particular piece of legislation. I am not sure. It is a judiciary issue. The vice chair is on the Judiciary Committee. It is an amendment that we were not able to pass in the managers' amendment. But as the vice chair and I said at the beginning of this process, we would like the Senate to function like it is designed, where every Member feels invested, and if they have a great idea, come down, introduce it as an amendment, debate it, and let your colleagues vote up or down against it. If we can't move forward with a process like that, then it is difficult to see how in a reasonable amount of time we are going to complete this agenda.

So I would only urge my colleague from Oregon that there is nothing to be scared about. This is a process we will go through, and a nongermane amendment, which I think this would be listed as—I look for my staff. It would be a nongermane amendment—requiring 60 votes, a threshold that the Senate designed to pass practically anything.

So I urge him to reconsider at some point, and I will make a similar unanimous consent request once he has had an opportunity to think about it. But also, we will work to see if in fact that amendment might be modified in a way that might make it a little more acceptable for the debate and for colleagues to vote on it.

With that, I yield the floor.

The PRESIDING OFFICER. The Senator from Utah.

Mr. HATCH. Madam President, as the Senate turns its focus to legislation related to the critical issue of our Nation's cyber security and in the light of Chinese President Xi Jinping's state visit last month, I would like to reflect on America's security in cyber space.

As the global economy becomes increasingly dependent on the Internet, the exponential increase in the number and scale of cyber attacks and cyber thefts are straining our relationship with international trading partners throughout the world. This is especially true for our important trade relationship with China. This year alone, the United States has experienced some of the largest cyber attacks in our Nation's history—many of which are believed to have been perpetrated by the Chinese. Just last February, hackers breached the customer records of the health insurance company Anthem Blue Cross Blue Shield. Many news sources reported that China was responsible for the attack. This cyber attack resulted in the theft of approximately 80 million customers' personally identifiable information, including Social Security numbers and information that can be used for identity theft.

In the early summer, cyber criminals also hacked United Airlines, compromising manifest data that detailed the movement of millions of Americans. According to the news media, China was again believed to have been responsible.

But the most devastating cyber attack this year was on the U.S. Government's Office of Personnel Management. This past June, sources report that the OPM data breach, considered the worst cyber intrusion ever perpetrated against the U.S. Government,

affected about 21.5 million Federal employees and contractors. Hackers successfully accessed sensitive personal information, including security clearance files, Social Security numbers, and information about employees' contacts and families. Again, China was the suspected culprit.

Most troubling, the OPM breach included over 19.7 million background investigation records for cleared U.S. Government employees. The exposure of this highly sensitive information not only puts our national security at risk but also raises concern that foreign governments may be keeping detailed databases on Federal workers and their associations.

I was pleased during the Chinese President's visit to Washington last month that President Obama expressed his ''very serious concerns about growing cyber threats'' and stated that the cyber theft of intellectual property and commercial trade secrets ''has to stop.'' President Obama and President Xi Jinping came to an agreement not to ''conduct or knowingly support'' cyber theft of intellectual property or commercial trade secrets.

Even so, Director of Intelligence James Clapper expressed doubts about the agreement in a hearing before the Senate Armed Services Committee last week. When Chairman MCCAIN asked Mr. Clapper if he was optimistic about the deal, he told members of the committee he was not. I add my skepticism of this agreement to the growing chorus of lawmakers, military leaders, and intelligence community personnel who have voiced similar concerns.

As Admiral Rogers, head of the National Security Agency and U.S. Cyber Command, has said, ''China is the biggest proponent of cyberattacks being waged against the U.S.'' We must do more to defend ourselves against this growing threat. Unfortunately, I have been disappointed in this administration's inability to protect our Federal computer systems from cyber intrusions and to hold criminals accountable for their participation in cyber attacks committed against the United States. Sadly, the cyber threats facing our Nation are not limited to China. Investigators believe Russia, North Korea, Iran, and several other nations have also launched cyber attacks against our government, U.S. citizens, and of course companies. These attacks are increasing both in severity and in number.

In April, Russian hackers accessed White House networks containing sensitive information, including emails sent and received by the President himself.

In May, hackers breached IRS servers to gain access to 330,000 American taxpayers' tax returns. That same month a fraudulent stock trader manipulated U.S. markets, costing the stock exchange an estimated $1 trillion in just 36 minutes. In July, it was reported that a Russian spear phishing attack shut down the Joint Chiefs of Staff email system for 11 days. Just 1 month ago, hackers stole the personal data of 15 million T-Mobile customers by breaching Experian, the company that processes credit checks for prospective customers. This stolen data includes names, birth dates, addresses, Social Security numbers, and credit card information.

These breaches have a serious and real cost for the victims. According to the Federal Trade Commission, the average identity fraud victim in 2012 incurred an average of $365 in losses. Incredibly, all of these high-profile breaches have occurred this year, making 2015 perhaps the worst year ever in terms of attacks on our national cyber security.

Prior to 2015, we also saw several high-profile breaches at large American corporations, including Target, Home Depot, Sony, and others. Our lack of effective cyber security policies and procedures threatens the safety of our people, the strength of our national defense, and the future of our economy. We must be more vigilant in reinforcing our cyber infrastructure to better defend ourselves against these attacks. In doing so, Congress must create a deterrent for those who seek to commit cyber attacks against our Nation. Our adversaries must know they will suffer dire consequences if they attack the United States. Finding a solution to this critical problem must be an urgent priority for the Senate.

I agree with Leader MCCONNELL that we must move forward in the Senate with legislation to improve our Nation's cyber security practices and policies. I am supportive of the objectives outlined in Chairman BURR and Vice Chairperson FEINSTEIN's bipartisan Cybersecurity Information Sharing Act, CISA.

I was pleased to see the Senate Select Committee on Intelligence pass the Burr-Feinstein CISA bill out of the committee by an overwhelming bipartisan vote of 14 to 1. This important legislation incentivizes and authorizes private sector companies to voluntarily share cyber threat information in real time that can be useful in detecting cyber attacks and in preventing future cyber intrusions.

I also commend Chairman BURR and Vice Chairman FEINSTEIN's efforts to include provisions in CISA to protect personal privacy, including a measure that prevents a user's personally identifiable information from being shared with government agencies. Additionally, CISA sets limits on information that can be collected or monitored by allowing information to be used only for cyber security purposes.

As the American economy grows ever more dependent on the Internet, I believe CISA represents an important first step in protecting our Nation's critical infrastructure from the devastating impact of cyber attacks. Congress must do more to adequately protect and secure America's presence in cyber space.

In light of recent revelations highlighting our Federal Government's inability to adequately protect and secure classified data and other sensitive information, I joined Senator CARPER, the ranking member of the Homeland Security and Governmental Affairs Committee, in introducing the Federal Computer Security Act.

The Hatch-Carper bill shines light on whether our Federal Government is using the most up-to-date cyber security practices and software to protect Federal computer systems and databases from both external cyber attackers and insider threats. Specifically, this legislation requires Federal agency inspectors general to report to Congress on the security practices and software used to safeguard classified and personally identifiable information on Federal computer systems themselves.

This bill also requires each Federal agency to submit a report to each respective congressional committee with oversight jurisdiction describing in detail to each committee which security access controls the agency is implementing to protect unauthorized access to classified and sensitive, personally identifiable information on government computers.

Requiring an accounting of each Federal agency's security practices, software, and technology is a logical first step in bolstering our Nation's cyber infrastructure. These reports will guide Congress in crafting legislation to prevent future large-scale data breaches and ensure that unauthorized users are not able to access classified and sensitive information.

Agencies should be employing multifactor authentication policies and should be implementing software to detect and monitor cyber security threats. They should also be using the most up-to-date technology and security controls. The future of our Nation's cyber security starts with our Federal Government practicing good cyber hygiene. In strengthening our security infrastructure, the Federal Government should be accountable to the American people, especially when cyber attacks affect millions of taxpayers.

I have heard from many constituents who have expressed concerns about the state of America's cyber security. I am honored to represent a State that is an emerging center of technological advancement and innovation, with the growing hub of computer companies expanding across a metropolitan area known as Silicon Slopes. The people of Utah recognize that our Nation's future depends on America's ability to compete in the digital area. They understand we must create effective cyber security policies so we can continue to lead the world in innovation and technology advancement.

I am pleased to announce that an amended version of the Federal Computer Security Act is included in Chairman BURR and Vice Chairman

FEINSTEIN's managers' package. I wish to express my appreciation to both the chairman and vice chairman for their willingness to work with me in fine-tuning this legislation. I appreciate it. I wish to also thank Chairman RON JOHNSON and Ranking Member TOM CARPER of the Homeland Security and Governmental Affairs Committee for their efforts in this endeavor as well.

In addition to broad bipartisan support in the Senate, the Federal Computer Security Act enjoys support from key industry stakeholders. Some of our Nation's largest computer security firms support the bill, including Symantec, Adobe, and CA Technologies. Several industry groups have also voiced their support, including the Business Software Alliance and the IT Alliance for the Public Sector.

I commend Intelligence Committee Chairman BURR and Vice Chairman FEINSTEIN for their leadership in managing this critical cyber security legislation. As Leader MCCONNELL works to restore the Senate to its proper function, I am grateful we have been able to consider this legislation in an open and transparent fashion. By reinstating the open amendment process, we have not only been able to vote on dozens of amendments this year, we have been able to refine legislation through robust consideration and debate. I think we voted on approximately 160-plus amendments so far this year, and they are about evenly split between Democrats and Republicans.

With the renewal of longstanding Senate practices, we are passing meaningful laws that will better serve the needs of the American people. May we build on the foundation of success as we work to improve this critically important Cybersecurity Information Sharing Act.

I wish to again thank the distinguished leaders of this Intelligence Committee. Having served 18 years on the Intelligence Committee, I really appreciate the work that both of them have done, especially on this bill, and I look forward to its passage.

With that, I yield the floor.

The PRESIDING OFFICER. The Senator from California.

Mrs. FEINSTEIN. Madam President, I thank the distinguished Senator from Utah for his words. They are much appreciated, as is his friendship as well. I think he knows that. I believe the chairman feels certainly as strongly if not more strongly than I do.

I rose to be able to make a brief statement about the sanctuary bill as in morning business, if that is possible.

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

STOP SANCTUARY POLICIES AND PROTECT AMERICANS BILL

Mrs. FEINSTEIN. Madam President, I voted against Senator VITTER's bill. I believe it goes much too far. My longer statement is in the RECORD, but I want to respond to some of what I heard today. I do believe we should ensure that there is a notification prior to release of a dangerous individual with a criminal record, just as Senator SCHUMER said on this floor. I do believe we could take a narrow action to do just that. We could focus on dangerous individuals and not on all undocumented immigrants who happen to be taken into State or local custody. We could require notification without threatening vital law enforcement and local government funding, as Senator VITTER's bill does.

I had an amendment prepared for the Judiciary Committee's consideration when the committee had scheduled the bill for markup over a series of weeks, but the committee canceled its markup, so we were on the floor today with a bill that has never been heard in full by the Judiciary Committee.

Senator VITTER's bill includes a notification requirement and a detention requirement. It is not limited to those who are dangerous or have particular criminal records. It would cover a farmworker who was detained for a broken taillight or a mother who was detained for similar reasons, taking her away from her children. This is a standard that could be abused in another administration, and it is potentially a huge unfunded mandate to impose on States and localities.

The bill would also impose lengthy criminal sentences at the Federal level for individuals coming across the border to see their families or to perform work that is vital to the economy of California and the Nation. For example, in California, virtually the majority, if not all, of the farmworkers are undocumented. It happens to be a fact. It is why the agriculture jobs bill was part of the immigration reform act which was before this body and passed this body and went to the House and had no action.

Although Members on the other side state that this bill has support among law enforcement, I will note that the Major Cities Chiefs Association, the Major County Sheriffs' Association, the Fraternal Order of Police, the United States Conference of Mayors, and the National League of Cities are opposed to this bill or have submitted letters opposing threats to Federal law enforcement funding over this issue.

So, bottom line, I do believe we should do something about the circumstance that led to the tragic murder of Kate Steinle, which occurred in my city and State, and the tragic murder of Marilyn Pharis, which happened in the middle part of my State. I will support a reasonable effort to do just that, but this is not a targeted effort. It is too broad, and so I opposed it. My full statement is in the RECORD, but because it was spoken about on the floor, I did want to add these words.

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

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Madam President, moving back to cyber security, we now have S. 754 before the Senate, and we have a managers' package that is pending. We have a number of amendments that have been accepted and incorporated in the managers' package. We have several amendments that we could not reach agreement on, but those Members have the opportunity to come to the Senate floor. The amendments are already pending. They can debate those amendments, and they can have a vote on their amendment. For Members who might just now be engaging or who have had an opportunity to further read the bill, there are still present opportunities to offer perfecting amendments.

Let me suggest to my colleagues that when the vice chairman and I started down this road, we knew we couldn't reach unanimous consent of every company in the country and every Member of Congress. It was our goal, and I think we are pretty close to it when we look at the numbers. But there will be companies that object to this bill for some reason that I might not recognize.

The vice chairman has said this and I have said it and I want to reiterate it another time: This bill is voluntary. It does not require any company in America to participate in this. It does not require any entity to turn over information to the Federal Government for purposes of the Federal Government partnering with that company to determine who hacked their system, who penetrated, and who exfiltrated personal data. If a company has made the determination that they don't want to support this bill for whatever reason, I am resigned to the fact that that is a debate between their customers and themselves. It is, in fact, their customers that have to question the actions of the company.

I can confidently tell my colleagues that Senator FEINSTEIN and I have done everything to make sure there is wholesome participation by companies on a voluntary basis. We see tremendous value in those parts of our government that are experts at processing attacks like this to be able to identify who did it and what tools were used but, more importantly, what software defensive mechanism we can put on our systems to limit any additional exfiltration of data and, more broadly, to the rest of the business community say: Here is an attack that is in progress. Here is the tool they are using. Here is how you defend your data.

Now, we leave open, if we pass it, that there may be a company that decides they don't support this legislation. They can still participate in this program. Do we think if they get a call from the Department of Homeland Security or from the National Security Agency saying ''Here is an attack that is happening; here is the tool they are using,'' they are going to look at their system and say ''Is it in our system?'' They get the benefit of still participating and partnering with the Federal Government, even though they didn't support the legislation.

I know over the next day or so the vice chairman and I will concentrate on sharing with Members what is actually in the managers' package. We don't leave it up to staff just to cover it.

Let me just briefly share 15 points that I would make about the managers' package.

No. 1, it eliminates the government's uses for noncyber crimes; in other words, a removal of the serious violent felonies.

No. 2, it limits the authorizations to share cyber threat information for cyber security purposes, period.

No. 3, it eliminates new FOIA exemptions. In other words, everybody is under the same FOIA regulations that existed prior to this legislation being enacted.

No. 4, it ensures defensive measures are properly limited. We can't get wild and put these things in places that government shouldn't be, regardless of what the threat is.

No. 5, it includes the Secretary of Homeland Security as coauthor—coauthor—of government-sharing guidelines. I think this is an incredibly important part. The individual who is in charge of Homeland Security, that Secretary, is actively involved in the guidelines that are written.

No. 6, it clarifies exceptions to the DHS portal entry point for the transfer of information.

No. 7, it adds a requirement that the procedures for government sharing include procedures for notifying U.S. persons whose personal information is known to have been shared in violation—in violation—of this act. In other words, if a company mistakenly transmits information, the government is required to notify that individual. But, additionally, the government is statutorily required not to disseminate that information to any other Federal agency once it comes in and is identified.

No. 8, it clarifies the real-time automated process for sharing through that DHS portal.

No. 9, it clarifies that private entities are not required to share information with the Federal Government or another private entity.

No. 10, it adds a Federal cyber security enhancement title.

No. 11, it adds a study on mobile device security.

No. 12, it adds a requirement for the Secretary of State to produce an international cyber space policy strategy.

No. 13, it adds a reporting provision concerning the apprehension and prosecution of international cyber criminals.

No. 14, it improves the contents of the biannual report on CISA's implementation. My colleagues might remember, as some have raised issues on this, they have said: Why are there not more reports? There are biannual reports on the implementation and how it is done.

No. 15, and last, is additional technical and conforming edits.

Now, we didn't get into detail. We will get into detail later, but I say that because if that has in any way triggered with somebody who felt they were opposed to the bill because of something they were told was in it, maybe it was covered by one of those 15 things that I just talked about. They are things that were brought to the attention of the vice chairman and me, and we sat down and looked at it. If we didn't feel as though it changed the intent of the bill—and we have always erred on the side of protecting personal data, of not letting this legislation extend outside of what it was intended to do. Where we have drawn the line is when we believed that the effort was to thwart the effectiveness of this legislation.

I will remind my colleagues one last time: This legislation does not prevent cyber attacks. This legislation is designed to minimize the loss of the personal data of the customers of the companies that are penetrated by these cyber actors.

As we stand here today, we have had some rather significant breaches within the United States. I remind my colleagues that just today it was proposed that a high school student has hacked the unclassified accounts, the personal email, of the Secretary of the Department of Homeland Security and the Director of the CIA. Is there anybody who really thinks that this is going to go away because we are having a debate in the Senate and in the Congress of the United States, that the people who commit these acts and go without any identification are going to quit? No. It is going to become more rampant and more rampant and more rampant. From the standpoint of 2 of 15 Members who are designated by the U.S. Senate and its leadership to, on behalf of the other 85, look at the most sensitive information that our country can accumulate about threats, as many threads of threats as we look at today on the security of the American people, I think I can speak for the vice chairman: We are just as concerned about the economic security of the United States based upon the threat that we are faced with from cyber actors here at home and, more importantly, around the world.

I urge my colleagues, if you have something to contribute, come to the floor and contribute it. If you have an amendment already pending, come to the floor and debate it and vote on it. Give us the ability to work through the great thoughts of all 100 Members, but recognize the fact that those individuals whom you have entrusted to represent you with the most sensitive information that exists in our country came to a 14-to-1 vote when they passed this originally out of the Intelligence Committee. That is because of how grave we see the threat and how real the attackers are.

I thank the vice chairman. She has been absolutely wonderful to work with through this process. We are going to have a long couple of days if we process all of this, but I am willing to be here as long as it takes so that we can move on to conference with the House.

I yield the floor.

The PRESIDING OFFICER. The Senator from California.

Mrs. FEINSTEIN. Madam President, I thank the chairman for those words. I have one little duty left.

AMENDMENT NO. 2626

Madam President, I call for the regular order with respect to Whitehouse amendment No. 2626.

The PRESIDING OFFICER. The amendment is now pending.

AMENDMENT NO. 2626, AS MODIFIED

Mrs. FEINSTEIN. I ask that the amendment be modified with the changes that are at the desk.

The PRESIDING OFFICER. The amendment is so modified.

The amendment, as modified, is as follows:

At the end, add the following:

SEC. ___. STOPPING THE SALE OF AMERICANS' FINANCIAL INFORMATION.

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. ___. SHUTTING DOWN BOTNETS.

(a) AMENDMENT.—Section 1345 of title 18, United States Code, is amended—

(1) in the heading, by inserting ''**and abuse**'' after ''**fraud**'';

(2) in subsection (a)—

(A) in paragraph (1)—

(i) in subparagraph (B), by striking ''or'' at the end;

(ii) in subparagraph (C), by inserting ''or'' after the semicolon; and

(iii) by inserting after subparagraph (C) the following:

''(D) violating or about to violate section 1030(a)(5) where such conduct has caused or would cause damage (as defined in section 1030) without authorization to 100 or more protected computers (as defined in section 1030) during any 1-year period, including by—

''(i) impairing the availability or integrity of the protected computers without authorization; or

''(ii) installing or maintaining control over malicious software on the protected computers that, without authorization, has caused or would cause damage to the protected computers;''; and

(B) in paragraph (2), by inserting '', a violation described in subsection (a)(1)(D),'' before ''or a Federal''; and

(3) by adding at the end the following:

''(c) A restraining order, prohibition, or other action described in subsection (b), if issued in circumstances described in subsection (a)(1)(D), may, upon application of the Attorney General—

''(1) specify that no cause of action shall lie in any court against a person for complying with the restraining order, prohibition, or other action; and

''(2) provide that the United States shall pay to such person a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in

complying with the restraining order, prohibition, or other action.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of section for chapter 63 is amended by striking the item relating to section 1345 and inserting the following:

''1345. Injunctions against fraud and abuse.''.

SEC. ___. AGGRAVATED DAMAGE TO A CRITICAL INFRASTRUCTURE COMPUTER.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer, if such damage results in (or, in the case of an attempted offense, would, if completed have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with such computer.

''(b) PENALTY.—Any person who violates subsection (a) shall, in addition to the term of punishment provided for the felony violation of section 1030, be fined under this title, imprisoned for not more than 20 years, or both.

''(c) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place any person convicted of a violation of this section on probation;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for the felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such violation to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, if such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.

''(d) DEFINITIONS.—In this section

''(1) the terms 'computer' and 'damage' have the meanings given the terms in section 1030; and

''(2) the term 'critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have catastrophic regional or national effects on public health or safety, economic security, or national security.''.

(b) TABLE OF SECTIONS.—The table of sections for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. ___. STOPPING TRAFFICKING IN BOTNETS.

(a) IN GENERAL.—Section 1030 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (7), by adding ''or'' at the end; and

(B) by inserting after paragraph (7) the following:

''(8) intentionally traffics in the means of access to a protected computer, if—

''(A) the trafficker knows or has reason to know the protected computer has been damaged in a manner prohibited by this section; and

''(B) the promise or agreement to pay for the means of access is made by, or on behalf of, a person the trafficker knows or has reason to know intends to use the means of access to—

''(i) damage the protected computer in a manner prohibited by this section; or

''(ii) violate section 1037 or 1343;'';

(2) in subsection (c)(3)—

(A) in subparagraph (A), by striking ''(a)(4) or (a)(7)'' and inserting ''(a)(4), (a)(7), or (a)(8)''; and

(B) in subparagraph (B), by striking ''(a)(4), or (a)(7)'' and inserting ''(a)(4), (a)(7), or (a)(8)'';

(3) in subsection (e)—

(A) in paragraph (11), by striking ''and'' at the end;

(B) in paragraph (12), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(13) the term 'traffic', except as provided in subsection (a)(6), means transfer, or otherwise dispose of, to another as consideration for the receipt of, or as consideration for a promise or agreement to pay, anything of pecuniary value.''; and

(4) in subsection (g), in the first sentence, by inserting '', except for a violation of subsection (a)(8),'' after ''of this section''.

Mrs. FEINSTEIN. I thank the Chair and yield the floor.

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

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

SANCTUARY CITIES BILL

Mr. PERDUE. Madam President, I rise to speak very briefly about the Stop Sanctuary Cities Act, which I was proud to cosponsor in the Senate. Simply put, this legislation protects American citizens from criminal illegal immigrants. Today, at least 340 cities across our country are choosing not to enforce our Nation's immigration laws. These sanctuary cities have become a safe haven for criminals who are not only in the United States illegally but also are committing additional crimes and repeatedly reentering trying our country after being deported. This summer we witnessed the tragic impact this lawlessness has on American citizens when Kate Steinle was murdered in San Francisco, a sanctuary city, by a felon living in our country illegally and who was previously deported five separate times. Three months prior to Kate's tragic death, the Department of Homeland Security actually asked San Francisco to detain her murderer, but the sanctuary city refused to cooperate and released the criminal back into the community. Had they not done that, had they turned that person over to Homeland Security as they were requested, Kate might still be with us.

This is unconscionable. I do not think I can overstate the importance of this Stop Sanctuary Cities Act to the American people and to the people of my home State of Georgia. The fact is that Kate Steinle did not have to die at the hands of a seven-time convicted felon and a five-time deportee. Kate and many others would not have died if our country had a functional immigration system and a government that actually enforces our laws.

This is why it is absolutely crucial that we stop sanctuary cities and address this illegal immigration crisis, which has also become a national security crisis. This bill would have done just that, and yet we were not able to even get it on the floor to have a debate. This is what drives people in my home State absolutely apoplectic. We want to get these bills to the floor, have an open debate, and let's let Americans see how we all vote on critical issues like this.

It is a very sad day, indeed, when this body cannot come together to stop rogue cities from breaking our Nation's laws, protecting the livelihood of American citizens, and support our law enforcement officials. I thank Senator VITTER and Chairman GRASSLEY for working closely with the victims' families and law enforcement to produce this legislation. I hope we can continue to debate this and get this bill back on the floor. I will keep fighting to stop this lawlessness and protect all Americans.

I yield the floor.

I suggest the absence of a quorum.

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

The legislative clerk proceeded to call the roll.

Mr. WHITEHOUSE. 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. WHITEHOUSE. Mr. President, I ask unanimous consent to speak as in morning business for up to 20 minutes.

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

CLIMATE CHANGE

Mr. WHITEHOUSE. Mr. President, last week the former head of the National Oceanic and Atmospheric Administration, Robert M. Hoyt, passed away at the age of 92. Dr. Hoyt served this Nation under five Presidents and pioneered the peaceful use of satellites to understand our weather and climate. He said:

> We do have environmental problems and they're serious ones, the preservation of species among them, but the climate is the environmental problem that's so pervasive in its effects on the society. . . . The climate is really the only environmental characteristic that can utterly change our society and our civilization.

That was in 1977. That same year, James F. Black, a top scientific researcher at the Exxon Corporation,

gave that company's executives a similar warning. ''[T]here is general scientific agreement,'' he told Exxon's Management Committee, ''that the most likely manner in which mankind is influencing the global climate is through carbon dioxide release from the burning of fossil fuels.'' According to emerging reports, Exxon executives kept that warning a closely guarded company secret for years.

I rise today for the 115th time to urge that we wake up to the threat of climate change. I rise in the midst of a decades-long purposeful corporate campaign of misinformation, which has held this Congress and this Nation back from taking meaningful action to prevent that utter change.

Scrutiny of the corporate campaign of misinformation intensifies, and scrutiny of the fossil fuel polluters behind it intensifies, and the regular cast of rightwing climate denier attack dogs have their hackles up.

On May 6 I gave a speech on the floor of the Senate. The speech compared the misinformation campaign by the fossil fuel industry about the dangers of carbon pollution to the tobacco industry's misinformation campaign about the dangers of its product. The relevance of that comparison is that the U.S. Department of Justice, under the civil provisions of the Federal racketeer influenced and corrupt organizations statute—RICO for short—brought an action against the tobacco industry. The United States alleged that the tobacco industry's misinformation campaign was fraudulent, and the United States won in a lengthy and thorough decision by U.S. District Judge Gladys Kessler.

You can go ahead and read them. DOJ's complaint and Judge Kessler's decision can be found at the Web sites of the Justice Department and the Public Health Law Center, respectively, and they are linked on my Web site, whitehouse.senate.gov/climate change. I will warn you that Judge Kessler's decision is a long one, but it makes good reading.

The comparison is strong. There are whole sections of the Department of Justice civil RICO complaint and whole sections of Judge Kessler's decision where you can remove the word ''tobacco'' and put in the word ''carbon'' and remove the word ''health'' and put in the word ''climate,'' and the parallel with the fossil fuel industry climate denial campaign is virtually perfect.

This is not an idea I just cooked up. Look at the academic work of Professor Robert Brulle of Drexel University and Professor Riley Dunlap of Oklahoma State University. Look at the investigative work of Naomi Oreskes' book ''Merchants of Doubt,'' David Michaels' book ''Doubt is Their Product,'' and Gerald Markowitz and David Rosner's book ''Deceit and Denial,'' describing this industry-backed machinery of deception.

Look at the journalistic work of Neela Banerjee, Lisa Song, David Hasemyer, and John Cushman, Jr., in the recent reporting of InsideClimate News about what Exxon knew about climate change versus the falsehoods that Exxon chose to tell the public. Look at a separate probe by journalists Sara Jerving, Katie Jennings, Masako Melissa Hirsch, and Susanne Rust in the Los Angeles Times.

From all their work, we know now that Exxon, for instance, knew about the effect of its carbon pollution as far back as the late 1970s but ultimately chose to fund a massive misinformation campaign rather than tell the truth. ''No corporation,'' said professor and climate change activist Bill McKibben, ''has ever done anything this big and this bad.''

Just today, the person who probably knows the most about the tobacco litigation, the assistant attorney general of the United States who prosecuted that case as a civil matter and won it in the U.S. District Court, Sharon Eubanks, said about the climate denial RICO idea: ''I think a RICO action is plausible and should be considered.''

This is how Judge Kessler depicted the culpable conduct of the tobacco industry in her decision in that case: ''Defendants have intentionally maintained and coordinated their fraudulent position on addiction and nicotine as an important part of their overall efforts to influence public opinion and persuade people that smoking is not dangerous.''

Now compare that to the findings of Dr. Brulle, whose research shines light on the dark-money campaigns that fund and support climate denial. This climate denial operation, to quote Dr. Brulle, is ''a deliberate and organized effort to misdirect the public discussion and distort the public's understanding of climate.''

The parallels between what the tobacco industry did and what the fossil fuel industry is doing now are so striking, I suggested in my speech of May 6, that it was worth a look, that civil discovery could reveal whether the fossil fuel industry's activities cross that same line into racketeering.

I said that again in an op-ed piece I wrote in the Washington Post on May 29 regarding the civil RICO action against tobacco. Oh my, what a caterwauling has ensued from the fossil fuel industry trolls. Here is a quick highlight reel of the tempest of rightwing invective.

One climate denier, Christopher Monckton, declared: ''Senator WHITEHOUSE is a fascist goon.''

Another denier compared me to Torquemada, the infamous torturer of the Inquisition.

The official Exxon responder got so excited about this suggestion that he used a word I am not even allowed to use on the Senate floor. He forgot rule No. 1 in crisis management: Don't lose your cool.

The rightwing Web site breitbart.com responded by calling me ''the preposterous Democrat senator for Rhode Island'' and saying the notion that there is an industry-led effort to mislead the American people about the harm caused by carbon pollution is ''a joke,'' a conspiracy theory on par with Area 51 or the faking of the Moon landing. Well, tell that to the tobacco industry.

Paul Gigot, the editorial page editor of the Wall Street Journal, said global warming concerns ''are based on computer models, not by actual evidence, not by actual evidence of what we've seen so far.'' Tell that to the scientists who measure the effects of climate change every day, particularly in our oceans.

The polluter-funded George C. Marshall Institute, a longtime climate denial outfit—and who knows how they got to take respectable George C. Marshall's name and slap it on the front of a climate denial industry front—they wrote that this was an attack on constitutional rights. Well, that kind of presumes the answer because there is no constitutional right to commit fraud.

Similarly, Calvin Beisner, founder of another phony baloney industry front called the Cornwall Alliance, said the same: The mere suggestion of considering this action represents a ''direct attack on the rights to freedom of speech and the press guaranteed by the First Amendment'' and is ''horrifically bad for science.'' Coming from a science-denial outfit, that concern for science is rich. Again, fraud is not protected by the First Amendment.

In the National Review, I was accused of wanting to launch ''organized crime investigations . . . against people and institutions that disagree with [me] about global warming'' in order to ''lock people up as Mafiosi.'' Crime? Lock people up? Let's remember, we are talking about civil RICO, not criminal. No one went to jail in the tobacco case. Investigating the organized climate denial scheme under civil RICO is not about putting people in jail.

Query why the National Review would mislead people about such an obvious fact, and they are not alone. The rightwing blogosphere has lit up with nonsense about how this is a criminal charge. Read the tobacco complaint. It is on the Department of Justice Web site. Even people who purport to be legal scholars are misleading folks that way. All a civil RICO case does is get people to actually have to tell the truth under oath in front of an actual impartial judge or jury and under cross-examination, which the Supreme Court has described as ''the greatest legal invention ever invented for the discovery of truth.'' No more spin and deception—but that is exactly the audience polluters and their allies cannot bear, so the flacks set off criminal smokescreens and launch fascist goon and Torquemada hysterics.

A few weeks ago, 20 scientists agreed with me and wrote a letter to Attorney General Lynch supporting the idea of using civil RICO. That was too much for the troll-in-chief for the fossil fuel

industry, the Wall Street Journal editorial page. The Wall Street Journal editorial page has long been an industry science-denial mouthpiece. They use the same playbook every time: one, deny the science; two, question the motives of reformers; and three, exaggerate the costs of reforms.

For example, when scientists warned that chlorofluorocarbons could break down the atmosphere's ozone layer, the Wall Street Journal ran editorials—for decades—devaluing the science, attacking scientists and reformers, and exaggerating the costs associated with regulating CFCs. It turns out they were dead wrong.

When acid rain was falling in the Northeast, the Wall Street Journal editorial page questioned the science, claimed the sulphur dioxide cleanup effort was driven by politics, and said fixing it carried a huge price tag. Ultimately, the Journal's editorial page, after years of this, had to recant and admit that the cap-and-trade program for sulphur dioxide ''saves about $700 million annually compared with the cost of traditional regulation and has been reducing emissions by four million tons annually.''

Now, on climate change, the Journal is back to the same pattern: Deny the science, question the motives of climate scientists, exaggerate the costs of tackling carbon pollution.

For decades, the Journal has been persistently publishing editorials against taking any action to prevent manmade climate change. On this, the editorial page said that by talking about civil RICO, I am trying to ''forcibly silence'' the denial apparatus. Forcibly silence? First of all, against the billions of the Koch brothers and the billions of ExxonMobil, fat chance that I have much ''force'' to use. And silence? I don't want them silent. I want them testifying in a forum where they have to tell the truth.

Is the Journal really saying that in a forum where climate deniers have to tell the truth, their only response would have to be silence? Making them tell the truth ''forcibly silences'' them? The only thing civil RICO silences is fraud.

By the way, the Journal editorial never mentions that the government won the civil RICO case against tobacco and on very similar facts. That would detract from the fable. Whom does the Journal cast as their victim in their fable? None other than Willie Soon, whom they said I singled out for—this is what they said—having ''published politically inconvenient research on changes in solar radiation.'' Politically inconvenient research.

Actually, what is inconvenient for Dr. Soon is that the New York Times reported that he got more than half his funding from big fossil fuel interests such as ExxonMobil and the Charles Koch Foundation to the tune of $1.2 million and didn't disclose it. Dr. Soon's research contracts even gave his industry backers a chance for comment and input before he published, and he referred to the papers he produced for them as ''deliverables.'' In case anyone listening doesn't know this, that is not how real science works. Of course, none of this sordid financial conflict is even mentioned by the Wall Street Journal editorial page. They would rather pretend that Dr. Soon is being singled out for ''politically inconvenient'' views. Please.

It gets better. In the editorial, the role of neutral expert commenting on all of this goes to Georgia Tech's Judith Curry. She offers the opinion that my ''demand . . . for legal persecution . . . represents a new low in the politicization of science.'' This is a particularly rich and conflict-riddled opinion, as Ms. Curry is herself a repeat anti-climate witness performing regularly in committees for Republicans here in Congress. Again, there is no mention of this interest of Ms. Curry's in the Wall Street Journal editorial.

The fossil fuel industry's climate denial machine rivals or exceeds that of the tobacco industry in size, scope, and complexity. Its purpose is to cast doubt about the reality of climate change in order to forestall moves toward cleaner fuels and to allow the Kochs and the Exxons of the world to continue making money at everybody else's expense. And the Wall Street Journal editorial page plays its part in this machine.

Even though it is only the editorial page and not the Journal's well-regarded newsroom, facts and logic are supposed to matter. Ignoring the successful tobacco litigation, omitting the salient fact of Dr. Soon being paid by the industry involved in his research, and bringing in a climate denier as their neutral voice without even disclosing that conflict—I would like to see the Wall Street Journal editorial page get that editorial by the editorial standards of their own newsroom.

So why all the histrionics on the far right? Why all the deliberate subterfuge between civil and criminal RICO? Why all the name-calling? Have we perhaps touched a little nerve? Have we made the hit a bit too close to home? Maybe a civil RICO case is indeed plausible and should be considered. Are the cracks in the dark castle of climate denial as it crumbles beginning to maybe rattle the occupants?

Whatever the motivation of the Wall Street Journal and other rightwing climate denial outfits, it is clearly long past time for this climate denial scheme to come in from the talk shows and the blogosphere and have to face the kind of truth-testing audience a civil RICO investigation could provide. It is time to let the facts take their place and let climate denial face that greatest legal engine ever invented for the discovery of truth.

Mr. President, 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.

CLOTURE MOTION

Mr. MCCONNELL. Mr. President, I send a cloture motion to the desk for the Burr-Feinstein amendment No. 2716.

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

The bill 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 amendment No. 2716 to S. 754, a bill to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

Mitch McConnell, John Cornyn, Johnny Isakson, Richard Burr, John McCain, Shelley Moore Capito, Orrin G. Hatch, John Thune, Chuck Grassley, Pat Roberts, John Barrasso, Jeff Flake, Lamar Alexander, Bill Cassidy, Deb Fischer, Susan M. Collins, Patrick J. Toomey.

CLOTURE MOTION

Mr. MCCONNELL. Mr. President, I send a cloture motion to the desk for the underlying bill, S. 754.

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

The bill 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 S. 754, an original bill to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

Mitch McConnell, John Cornyn, Johnny Isakson, Richard Burr, John McCain, Shelley Moore Capito, Orrin G. Hatch, John Thune, Chuck Grassley, Pat Roberts, John Barrasso, Jeff Flake, Lamar Alexander, Bill Cassidy, Deb Fischer, Susan M. Collins, Patrick J. Toomey.

MORNING BUSINESS

Mr. MCCONNELL. Mr. 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.

VOTE EXPLANATION

Mr. RUBIO. Mr. President, on September 28, 2015, I was unable to vote on the motion to proceed to a short-term budget—continuing resolution—that, among other measures, denied taxpayer funding to Planned Parenthood. I would have voted no.

On September 30, 2015, I was unable to vote on final passage of a short-term budget—continuing resolution—to fund

the government through December 11, 2015, including taxpayer funding for Planned Parenthood. I would have voted no.

REMEMBERING JEFFREY A. MATHIAS

Mr. MARKEY. Mr. President, I am a cosponsor of a resolution the Senate is likely to pass this evening honoring the lives of the 33 crew members aboard the *El Faro* which sank near the Bahamas during Hurricane Joaquin earlier this month.

I want to take this opportunity to express my deepest sympathy and sincere condolences to the family of *El Faro* crewman Jeffrey A. Mathias of Kingston, MA. He was just 42 years old.

Jeff loved the sea. When he attended Tabor Academy, he learned how to sail aboard the school's sailing ship the *Tabor Boy*. Jeff followed his passion to the prestigious Massachusetts Maritime Academy, where in 1996 he graduated with a degree in marine engineering. Upon graduation, he worked at Seamass and then Altran, where he was involved with nuclear power plants. In 1998, he landed his dream job on a cargo vessel.

Jeff sailed to Africa, Europe, North Korea, Alaska, Hawaii, California, and the Caribbean. He reached the officer's position of chief engineer and was responsible for shaft repairs on many vessels.

Jeff leaves his beloved wife, Jennifer Brides Mathias; his 3 adored children, daughters Hayden, 7, Heidi, 5, and son, Caleb, 3, all of Kingston. He also leaves behind his parents, J. Barry and Lydia Jones Mathias, of Kingston and his brother John.

Another son of Massachusetts who loved the sea was President John F. Kennedy. He famously stated, ''I really don't know why it is that all of us are so committed to the sea, except I think it's because in addition to the fact that the sea changes, and the light changes, and ships change, it's because we all came from the sea. And it is an interesting biological fact that all of us have in our veins the exact same percentage of salt in our blood that exists in the ocean, and, therefore, we have salt in our blood, in our sweat, in our tears. We are tied to the ocean. And when we go back to the sea—whether it is to sail or to watch it—we are going back from whence we came.''

I also offer my condolences to the family, friends, and loved ones of every member of the *El Faro* crew.

ADDITIONAL STATEMENTS

TRIBUTE TO SERGEANT MICHAELA BOUSHEY AND STAFF SERGEANT SHAYNE BOUSHEY

• Mr. DAINES. Mr. President, I wish to recognize SGT Michaela Boushey and SSG Shayne Boushey as Montanans of the Week. These two soldiers represent not only the best that Montana has to offer, but the best this country has to offer.

SGT Michaela Boushey served in the Montana Army National Guard for 8 years. For 4 years, she served in the 112th Security and Support Detachment Aviation Unit whose mission is to protect our borders, collect and transmit intelligence, and to provide support for the Department of Justice. Michaela's commitments and service to our country has never faltered, and we are so grateful for her service, sacrifice, and loyalty to our great Nation.

Her husband, SSG Shayne Boushey, was deployed with both the infantry battalion and the military police company. During his deployment to Afghanistan, Shayne and his team were targeted by Taliban forces. When a suicide bomber detonated himself, 6 were killed and 13 were seriously wounded. Shayne's fast thinking, bravery, and resolve in this life-threatening situation saved the lives of many in his team.

We owe our freedom to these soldiers and the thousands of American servicemembers like them. It is with the humblest gratitude that I thank them for their courage and unwavering loyalty.•

TRIBUTE TO CHASE DELLWO

• Mr. DAINES. Mr. President, today I would like to highlight an incredibly courageous Montanan and a man very dear to my staff and me: Chase Dellwo. Chase is a strong example of the courage, bravery, and quick thinking that sets Montanans apart.

Chase Dellwo, like myself and many other Montanans, is a hunter. In recent weeks, however, Chase showed resolve that many could never achieve. While bow hunting with his brother recently, Chase climbed up a narrow creek expecting to drive a herd of elk toward his waiting brother.

Having been focused on the elk, Chase did not notice the sleeping grizzly bear 3 feet from where he stood. Startling the now awake animal, Chase soon found himself head to head with this 400-pound bear. Chase recounts later that there was no time for him to draw his weapon back before he had been knocked off his feet and bit on the top and back of his head.

With his eye swollen shut, part of his scalp hanging over his eye, and blood pouring from his wounds, he suffered through the animal's repeated assaults. This attack in normal circumstances would have been the end of a hunter's life, but not in the case of Chase Dellwo. Mid-attack, Chase remembered an article his grandmother had sent him about large animals having terrible gag reflexes.

This quick thinking led him to plunge his arm down the animal's throat, enacting the bear's gag reflex, and subsequently scaring the animal away. Despite incredible disorientation, he found his way to his brother and was in turn rushed to the nearest hospital.

After undergoing multiple hours of surgery to fix his many lacerations, Chase sat with his wife, defending the bear, saying that it had been just as startled as he had. His many injuries led to multiple stitches, staples, and a hospital stay, but this 26-year-old remains alive and has encouraged Montana residents to be more aware of the animals that share their land.

I commend Chase on his courage and smarts that saved his life and wish him luck on both his recovery and the upcoming hunting season.•

REMEMBERING BETTE BAILLY

• Mr. GARDNER. Mr. President, I wish to honor the life of Bette Bailly from Burlington, CO, who passed away earlier this month after serving nearly 50 years in the broadcast industry.

Bette was an inspiration to others in her professional life and in her community. She was due to celebrate 50 years of dedicated service at her station, KNAB–AM, in just 2 years' time and was honored and recognized with numerous awards throughout her career. As a businesswoman, Bette was hard-charging and took a no-nonsense approach to broadcasting. Her tenacity was well known and respected throughout Northeastern Colorado.

Bette was also devoted to the Burlington community. She volunteered her time at the Burlington Chamber of Commerce, the Rotary Club, numerous local boards, and her church.

Undoubtedly, Bette will be missed dearly by her family, her community, and the State of Colorado. We will never forget her contributions to local broadcasting.•

RECOGNIZING BERKLEY SCHOOLS

• Mr. PETERS. Mr. President, I wish to recognize the 175th Anniversary of Berkley Schools. I appreciate the opportunity to recognize this truly significant milestone in the history of the Berkley School District and the city of Berkley, MI. I am proud of Berkley's enduring commitment to providing quality public education and wish it many more decades of successful service to its students and their families.

Throughout its history, the Berkley School District has set the benchmark in public education, ensuring its students are prepared for success, both as individuals and leaders in an increasingly global community. The district's continued dedication to academics is apparent in its recognition by North Central Accreditation, as well as the many honors its students have received in marketing, communications, literacy and poetry, robotics, and video production. Berkley High School boasts 21 advanced placement and college level courses—more than any other traditional high school campus—and provides the highest math curriculum of any high school in Michigan's Oakland County. Additionally, the district's Norup International

School is the United States only K–8 International Baccalaureate program housed on one campus. It is no surprise Berkley High School enjoys a 98 percent graduation rate, with nearly 100 percent of those graduates enrolling in colleges and universities.

In addition to ensuring its students' success in the classroom, the Berkley School District provides an opportunity for students to participate in a wide variety of varsity sports, clubs, and student organizations. From football and softball, to rugby and skiing, students can compete for the Berkley Bears throughout the year. Students also entertain as members of the high school's marching band, symphonic band, concert band, and jazz band, as well as with its three choirs and theater program. I applaud the Berkley School District for providing opportunities for students to explore art, music, and literature.

Berkley had been associated with education for nearly a century when the city was incorporated in 1932. The Berkley School was mentioned as part of the Royal Oak Township School District No. 7 in 1840. It was housed in the Blackmon School, at the corner of Coolidge and Catalpa, from 1840 until a new school building was established in 1901. The new building, named South School, was located at the northeast corner of Coolidge and 11 Mile Road until it was converted into a dormitory for teachers in 1920. The district's growth was swift. In 1921, the district built Angell School, a four-room building, on Bacon Street. Four years later, in 1925, the district added two more schools, Pattengill and Burton, which were occupied before they were even completed.

Despite its success, the Berkley School District was not immune to the hardships of the Great Depression. In January 1930, all pupils were placed on half days, half of the faculty was dismissed, bus service was eliminated, and the gym was closed. The following year, the district was forced to close Burton and Pattengill schools. Fortunately, both schools were reopened in time for the ''baby boom'' that followed the end of World War II. As the district's population grew, Berkley High School opened in 1949, followed by Tyler and Oxford Schools in 1951; Hamilton School in 1952; and the district's two junior high schools, Anderson and Norup, in 1956 and 1957.

Today, the Berkley School District continues to be a leader in providing excellent public education in the State of Michigan. It serves as an example of how community-driven, quality education can not only enrich the lives of students, but also drive the growth and quality of life in the surrounding community for generations. I am pleased to help celebrate the 175th Anniversary of Berkley Schools and wish it many more decades of successful service to its students and their families.●

RECOGNIZING THE UNIVERSITY OF CENTRAL FLORIDA'S COLLEGIATE CYBER DEFENSE CLUB

● Mr. RUBIO. Mr. President, as October marks Cyber Security Awareness Month, I wish to recognize the University of Central Florida, UCF, Collegiate Cyber Defense Club on winning the 2015 National Collegiate Cyber Defense Competition's Alamo Cup for a second year in a row in April 2015. This achievement not only exemplifies the boundless educational opportunities provided by UCF, but also demonstrates how students in Florida are leading the next generation of growth and development in increasingly vital 21st century industries.

The UCF Collegiate Cyber Defense Club, also known as Hack@UCF was founded in 2012 and today has 200 members that represent the university in cyber competitions around the Nation. Most notably, Hack@UCF annually competes in the National Collegiate Cyber Defense Competition, CCDC. In partnership with the Center for Infrastructure Assurance and Security, CIAS, at the University of Texas at San Antonio, the CCDC started in 2005 to provide educational institutions with a controlled environment to further educate and assess the future generation's skills in combatting cyber attacks. This year, the competition challenged 2,400 undergraduate and graduate students representing 200 colleges and universities to operate and maintain a mock business, while continuously defending against cyber attacks created by government and industry experts.

I am proud that the talented students of UCF were able to stand out as the best collegiate team during the competition for the past 2 years. As our Nation will continue to face the threat of cyber attacks on our economy, businesses, and national security, it is critical to promote and invest in educational programs that empower students and provide them with the necessary tools to be successful in this industry.

It is an honor to congratulate all members of the UCF Collegiate Cyber Defense Club on this achievement. I hope it will inspire other students in the State of Florida and across the Nation to get involved in the cyber security industry. I wish the group an abundance of success in the future and the best of luck in next year's competition.●

TRIBUTE TO DR. FRANK FIERMONTE

● Mr. SANDERS. Mr. President, I wish to recognize Dr. Frank Fiermonte, a physician from Orleans, VT, who cared for the people of Vermont's North Country with distinction for many years. As Vermont's Northland Journal prepares to publish the final installment of a series on Dr. Fiermonte, I want to join in recognizing his service to Vermont.

Dr. Fiermonte was a true ''country doctor'' who was willing to travel long distances to see his patients at all hours and in all seasons. I have heard Frank tell many an anecdote about how, after a home visit to a rural area, family and friends of the patient had to help him get his car unstuck during mud season or dug out from a snow bank in the winter.

Like many country doctors, he served a vast area, encompassing not just his hometown of Derby, but also a wide swath of Orleans and Essex Counties and even across the border into Quebec. Yet he intimately knew all of the families he served, which sometimes spanned several generations. The stories from North Country residents in the Northland Journal make it clear that Dr. Fiermonte made a tremendous impact on the community. This quote from a former Derby resident stands out in particular: ''Dr. Fiermonte was a godsend to the Derby area. He was always available day or night.''

What always strikes me most about Frank is how personal the practice of medicine was for him. In today's modern world, health care can sometimes be a very impersonal experience. In fact, there is much discussion in Vermont and Washington about returning to a more patient-centered system. We would do well to learn from people like Dr. Frank Fiermonte and his contemporaries, who are the embodiment of that ideal. Motivated by the desire to serve his community and deliver the best care possible, for Dr. Fiermonte, it was all about the patient.

Dr. Frank Fiermonte has earned my deepest respect, and I thank him for his years of service to the North Country.●

MEASURES PLACED ON THE CALENDAR

The following bills were read the second time, and placed on the calendar:

S. 2181. A bill to provide guidance and priorities for Federal Government obligations in the event that the debt limit is reached.

S. 2182. A bill to cut, cap, and balance the Federal budget.

S. 2183. A bill to reauthorize and reform the Export-Import Bank of the United States, and for other purposes.

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. RUBIO (for himself and Mr. CARDIN):

S. 2184. A bill to direct the President to establish guidelines for United States foreign development and economic assistance programs, and for other purposes; to the Committee on Foreign Relations.

By Ms. HEITKAMP (for herself, Ms. AYOTTE, Ms. COLLINS, Mrs. CAPITO, Mr. HOEVEN, Mrs. FEINSTEIN, Ms. KLOBUCHAR, Ms. HIRONO, and Mrs. GILLIBRAND):

S. 2185. A bill to require the Secretary of the Treasury to mint coins in recognition of the fight against breast cancer; to the Committee on Banking, Housing, and Urban Affairs.

By Mr. RUBIO:

S. 2186. A bill to provide the legal framework necessary for the growth of innovative private financing options for students to fund postsecondary education, and for other purposes; to the Committee on Finance.

SUBMISSION OF CONCURRENT AND SENATE RESOLUTIONS

The following concurrent resolutions and Senate resolutions were read, and referred (or acted upon), as indicated:

By Mr. PAUL (for himself and Mr. ROBERTS):

S. Res. 290. A resolution expressing the sense of the Senate that any protocol to, or other agreement regarding, the United Nations Framework Convention on Climate Change of 1992, negotiated at the 2015 United Nations Climate Change Conference in Paris will be considered a treaty requiring the advice and consent of the Senate; to the Committee on Foreign Relations.

ADDITIONAL COSPONSORS

S. 134

At the request of Mr. WYDEN, the name of the Senator from Vermont (Mr. SANDERS) was added as a cosponsor of S. 134, a bill to amend the Controlled Substances Act to exclude industrial hemp from the definition of marihuana, and for other purposes.

S. 314

At the request of Mr. GRASSLEY, the names of the Senator from Montana (Mr. TESTER) and the Senator from Kansas (Mr. MORAN) were added as cosponsors of S. 314, a bill to amend title XVIII of the Social Security Act to provide for coverage under the Medicare program of pharmacist services.

S. 370

At the request of Mrs. FEINSTEIN, the name of the Senator from Nevada (Mr. HELLER) was added as a cosponsor of S. 370, a bill to require breast density reporting to physicians and patients by facilities that perform mammograms, and for other purposes.

S. 403

At the request of Ms. KLOBUCHAR, the name of the Senator from North Dakota (Ms. HEITKAMP) was added as a cosponsor of S. 403, a bill to revise the authorized route of the North Country National Scenic Trail in northeastern Minnesota and to extend the trail into Vermont to connect with the Appalachian National Scenic Trail, and for other purposes.

S. 613

At the request of Mrs. GILLIBRAND, the names of the Senator from Washington (Mrs. MURRAY) and the Senator from Montana (Mr. TESTER) were added as cosponsors of S. 613, a bill to amend the Richard B. Russell National School Lunch Act to improve the efficiency of summer meals.

S. 637

At the request of Mr. CRAPO, the name of the Senator from North Dakota (Mr. HOEVEN) 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. 851

At the request of Mr. THUNE, the name of the Senator from New Hampshire (Ms. AYOTTE) was added as a cosponsor of S. 851, a bill to promote neutrality, simplicity, and fairness in the taxation of digital goods and digital services.

S. 1013

At the request of Mr. SCHUMER, the name of the Senator from Connecticut (Mr. MURPHY) was added as a cosponsor of S. 1013, a bill to amend title XVIII of the Social Security Act to provide for coverage and payment for complex rehabilitation technology items under the Medicare program, and for other purposes.

S. 1077

At the request of Mr. BENNET, the name of the Senator from Indiana (Mr. DONNELLY) was added as a cosponsor of S. 1077, a bill to provide for expedited development of and priority review for breakthrough devices.

S. 1082

At the request of Mr. INHOFE, his name was added as a cosponsor of S. 1082, a bill to amend title 38, United States Code, to provide for the removal or demotion of employees of the Department of Veterans Affairs based on performance or misconduct, and for other purposes.

S. 1315

At the request of Mr. ENZI, the names of the Senator from Kansas (Mr. MORAN) and the Senator from Montana (Mr. TESTER) were added as cosponsors of S. 1315, a bill to protect the right of law-abiding citizens to transport knives interstate, notwithstanding a patchwork of local and State prohibitions.

S. 1375

At the request of Mr. DURBIN, the name of the Senator from New Jersey (Mr. BOOKER) 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. 1394

At the request of Mr. MERKLEY, the name of the Senator from Washington (Ms. CANTWELL) was added as a cosponsor of S. 1394, a bill to amend the Federal Water Pollution Control Act to establish within the Environmental Protection Agency a Columbia River Basin Restoration Program.

S. 1493

At the request of Mr. ISAKSON, the name of the Senator from Kansas (Mr. ROBERTS) was added as a cosponsor of S. 1493, a bill to provide for an increase, effective December 1, 2015, in the rates of compensation for veterans with service-connected disabilities and the rates of dependency and indemnity compensation for the survivors of certain disabled veterans, and for other purposes.

S. 1520

At the request of Ms. KLOBUCHAR, the names of the Senator from Illinois (Mr. DURBIN) and the Senator from Illinois (Mr. KIRK) were added as cosponsors of S. 1520, a bill to protect victims of stalking from violence.

S. 1539

At the request of Mrs. MURRAY, the name of the Senator from Oregon (Mr. WYDEN) was added as a cosponsor of S. 1539, a bill to amend the Richard B. Russell National School Lunch Act to establish a permanent, nationwide summer electronic benefits transfer for children program.

S. 1559

At the request of Ms. AYOTTE, the names of the Senator from Connecticut (Mr. BLUMENTHAL), the Senator from Wisconsin (Ms. BALDWIN), the Senator from Massachusetts (Mr. MARKEY) and the Senator from Maine (Ms. COLLINS) were added as cosponsors of S. 1559, a bill to protect victims of domestic violence, sexual assault, stalking, and dating violence from emotional and psychological trauma caused by acts of violence or threats of violence against their pets.

S. 1624

At the request of Ms. STABENOW, the name of the Senator from Iowa (Mr. GRASSLEY) was added as a cosponsor of S. 1624, a bill to provide predictability and certainty in the tax law, create jobs, and encourage investment.

S. 1686

At the request of Ms. BALDWIN, the name of the Senator from California (Mrs. FEINSTEIN) was added as a cosponsor of S. 1686, a bill to amend the Internal Revenue Code of 1986 to provide for the proper tax treatment of personal service income earned in passthru entities.

S. 1766

At the request of Mr. SCHATZ, the names of the Senator from Delaware (Mr. CARPER) and the Senator from Missouri (Mrs. MCCASKILL) were added as cosponsors of S. 1766, a bill to direct the Secretary of Defense to review the discharge characterization of former members of the Armed Forces who were discharged by reason of the sexual orientation of the member, and for other purposes.

S. 1767

At the request of Mr. ISAKSON, the name of the Senator from Indiana (Mr. DONNELLY) was added as a cosponsor of S. 1767, a bill to amend the Federal Food, Drug, and Cosmetic Act with respect to combination products, and for other purposes.

S. 1789

At the request of Mr. RUBIO, the names of the Senator from Oregon (Mr. MERKLEY), the Senator from South Dakota (Mr. ROUNDS) and the Senator

from Connecticut (Mr. MURPHY) were added as cosponsors of S. 1789, a bill to improve defense cooperation between the United States and the Hashemite Kingdom of Jordan.

S. 1801

At the request of Ms. KLOBUCHAR, the name of the Senator from Montana (Mr. TESTER) was added as a cosponsor of S. 1801, a bill to amend the Internal Revenue Code of 1986 to treat certain farming business machinery and equipment as 5-year property for purposes of depreciation.

S. 1831

At the request of Mr. TOOMEY, the names of the Senator from Wisconsin (Ms. BALDWIN) and the Senator from New Mexico (Mr. UDALL) were added as cosponsors of S. 1831, a bill to revise section 48 of title 18, United States Code, and for other purposes.

S. 1833

At the request of Mr. CASEY, the name of the Senator from Rhode Island (Mr. REED) was added as a cosponsor of S. 1833, a bill to amend the Richard B. Russell National School Lunch Act to improve the child and adult care food program.

S. 1882

At the request of Mr. CARDIN, the name of the Senator from California (Mrs. FEINSTEIN) was added as a cosponsor of S. 1882, a bill to support the sustainable recovery and rebuilding of Nepal following the recent, devastating earthquakes near Kathmandu.

S. 1926

At the request of Ms. MIKULSKI, the names of the Senator from Massachusetts (Mr. MARKEY) and the Senator from New York (Mrs. GILLIBRAND) were added as cosponsors of S. 1926, a bill to ensure access to screening mammography services.

S. 1931

At the request of Mr. MORAN, the name of the Senator from Minnesota (Mr. FRANKEN) was added as a cosponsor of S. 1931, a bill to reaffirm that certain land has been taken into trust for the benefit of certain Indian tribes.

S. 1944

At the request of Mr. SULLIVAN, the name of the Senator from Utah (Mr. LEE) was added as a cosponsor of S. 1944, a bill to require each agency to repeal or amend 1 or more rules before issuing or amending a rule.

S. 2002

At the request of Mr. CORNYN, the names of the Senator from Missouri (Mr. BLUNT) and the Senator from Kansas (Mr. ROBERTS) were added as cosponsors of S. 2002, a bill to strengthen our mental health system and improve public safety.

S. 2028

At the request of Mr. PAUL, the name of the Senator from Maine (Ms. COLLINS) was added as a cosponsor of S. 2028, a bill to amend the Federal Credit Union Act, to advance the ability of credit unions to promote small business growth and economic development opportunities, and for other purposes.

S. 2034

At the request of Mr. TOOMEY, the names of the Senator from Wyoming (Mr. BARRASSO), the Senator from Arkansas (Mr. COTTON), the Senator from Idaho (Mr. RISCH), the Senator from Idaho (Mr. CRAPO), the Senator from Wisconsin (Mr. JOHNSON), the Senator from Nebraska (Mrs. FISCHER), the Senator from Louisiana (Mr. CASSIDY), the Senator from Utah (Mr. LEE), the Senator from Arizona (Mr. MCCAIN), the Senator from Montana (Mr. DAINES), the Senator from Oklahoma (Mr. INHOFE) and the Senator from Utah (Mr. HATCH) were added as cosponsors of S. 2034, a bill to amend title 18, United States Code, to provide additional aggravating factors for the imposition of the death penalty based on the status of the victim.

S. 2042

At the request of Mrs. MURRAY, the name of the Senator from Oregon (Mr. MERKLEY) 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. 2067

At the request of Mr. WICKER, the names of the Senator from New York (Mrs. GILLIBRAND) and the Senator from Delaware (Mr. CARPER) were added as cosponsors of S. 2067, a bill to establish EUREKA Prize Competitions to accelerate discovery and development of disease-modifying, preventive, or curative treatments for Alzheimer's disease and related dementia, to encourage efforts to enhance detection and diagnosis of such diseases, or to enhance the quality and efficiency of care of individuals with such diseases.

S. 2136

At the request of Mr. VITTER, the name of the Senator from Delaware (Mr. COONS) was added as a cosponsor of S. 2136, a bill to establish the Regional SBIR State Collaborative Initiative Pilot Program, and for other purposes.

S. 2145

At the request of Mr. LEAHY, the names of the Senator from Illinois (Mr. DURBIN), the Senator from New Hampshire (Mrs. SHAHEEN) and the Senator from Connecticut (Mr. MURPHY) were added as cosponsors of S. 2145, a bill to make supplemental appropriations for fiscal year 2016.

S. 2146

At the request of Mr. VITTER, the names of the Senator from Nebraska (Mrs. FISCHER) and the Senator from South Carolina (Mr. SCOTT) were added as cosponsors of 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.

S. 2148

At the request of Mr. WYDEN, the names of the Senator from Massachusetts (Ms. WARREN), the Senator from California (Mrs. BOXER) and the Senator from Connecticut (Mr. MURPHY) were added as cosponsors 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. 2163

At the request of Ms. KLOBUCHAR, the name of the Senator from West Virginia (Mrs. CAPITO) was added as a cosponsor of S. 2163, a bill to amend title 23, United States Code, to direct the Secretary of Transportation to require that broadband conduits be installed as a part of certain highway construction projects, and for other purposes.

S. RES. 282

At the request of Mrs. SHAHEEN, the name of the Senator from Maine (Ms. COLLINS) was added as a cosponsor of S. Res. 282, a resolution supporting the goals and ideals of American Diabetes Month.

SUBMITTED RESOLUTIONS

SENATE RESOLUTION 290—EXPRESSING THE SENSE OF THE SENATE THAT ANY PROTOCOL TO, OR OTHER AGREEMENT REGARDING, THE UNITED NATIONS FRAMEWORK CONVENTION ON CLIMATE CHANGE OF 1992, NEGOTIATED AT THE 2015 UNITED NATIONS CLIMATE CHANGE CONFERENCE IN PARIS WILL BE CONSIDERED A TREATY REQUIRING THE ADVICE AND CONSENT OF THE SENATE

Mr. PAUL (for himself and Mr. ROBERTS) submitted the following resolution; which was referred to the Committee on Foreign Relations:

S. RES. 290

Whereas the 105th Congress passed S. Res. 98, which required the Kyoto Protocol to the United Nations Framework Convention on Climate Change of 1992 to receive Senate advice and consent prior to ratification: Now, therefore, be it

Resolved, That it is the sense of the Senate that any protocol to, or other agreement regarding, the United Nations Framework Convention on Climate Change of 1992, negotiated at the 2015 United Nations Climate Change Conference in Paris will be considered a treaty requiring the advice and consent of the Senate.

AMENDMENTS SUBMITTED AND PROPOSED

SA 2713. Mr. WHITEHOUSE (for himself and Mr. GRAHAM) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table.

SA 2714. Mr. BARRASSO submitted an amendment intended to be proposed by him to the bill S. 209, to amend the Indian Tribal Energy Development and Self-Determination Act of 2005, and for other purposes; which was ordered to lie on the table.

SA 2715. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table.

SA 2716. Mr. BURR (for himself and Mrs. FEINSTEIN) proposed an amendment to the bill S. 754, supra.

SA 2717. Mr. UDALL (for himself, Mrs. SHAHEEN, Mr. TESTER, and Mr. MERKLEY) submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2718. Mr. UDALL (for himself, Mrs. SHAHEEN, Mr. TESTER, and Mr. MERKLEY) submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2719. Mr. ALEXANDER submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

TEXT OF AMENDMENTS

SA 2713. Mr. WHITEHOUSE (for himself and Mr. GRAHAM) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

SEC. ___. STOPPING THE SALE OF AMERICANS' FINANCIAL INFORMATION.

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. ___. SHUTTING DOWN BOTNETS.

(a) AMENDMENT.—Section 1345 of title 18, United States Code, is amended—

(1) in the heading, by inserting ''**and abuse**'' after ''**fraud**'';

(2) in subsection (a)—

(A) in paragraph (1)—

(i) in subparagraph (B), by striking ''or'' at the end;

(ii) in subparagraph (C), by inserting ''or'' after the semicolon; and

(iii) by inserting after subparagraph (C) the following:

''(D) violating or about to violate section 1030(a)(5) where such conduct has caused or would cause damage (as defined in section 1030) without authorization to 100 or more protected computers (as defined in section 1030) during any 1-year period, including by—

''(i) impairing the availability or integrity of the protected computers without authorization; or

''(ii) installing or maintaining control over malicious software on the protected computers that, without authorization, has caused or would cause damage to the protected computers;''; and

(B) in paragraph (2), by inserting '', a violation described in subsection (a)(1)(D),'' before ''or a Federal''; and

(3) by adding at the end the following:

''(c) A restraining order, prohibition, or other action described in subsection (b), if issued in circumstances described in subsection (a)(1)(D), may, upon application of the Attorney General—

''(1) specify that no cause of action shall lie in any court against a person for complying with the restraining order, prohibition, or other action; and

''(2) provide that the United States shall pay to such person a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in complying with the restraining order, prohibition, or other action.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of section for chapter 63 is amended by striking the item relating to section 1345 and inserting the following:

''1345. Injunctions against fraud and abuse.''.

SEC. ___. AGGRAVATED DAMAGE TO A CRITICAL INFRASTRUCTURE COMPUTER.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer, if such damage results in (or, in the case of an attempted offense, would, if completed have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with such computer.

''(b) PENALTY.—Any person who violates subsection (a) shall, in addition to the term of punishment provided for the felony violation of section 1030, be fined under this title, imprisoned for not more than 20 years, or both.

''(c) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place any person convicted of a violation of this section on probation;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for the felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such violation to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, if such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.

''(d) DEFINITIONS.—In this section

''(1) the terms 'computer' and 'damage' have the meanings given the terms in section 1030; and

''(2) the term 'critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have catastrophic regional or national effects on public health or safety, economic security, or national security.''.

(b) TABLE OF SECTIONS.—The table of sections for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. ___. STOPPING TRAFFICKING IN BOTNETS.

(a) IN GENERAL.—Section 1030 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (7), by adding ''or'' at the end; and

(B) by inserting after paragraph (7) the following:

''(8) intentionally traffics in the means of access to a protected computer, if—

''(A) the trafficker knows or has reason to know the protected computer has been damaged in a manner prohibited by this section; and

''(B) the promise or agreement to pay for the means of access is made by, or on behalf of, a person the trafficker knows or has reason to know intends to use the means of access to—

''(i) damage the protected computer in a manner prohibited by this section; or

''(ii) violate section 1037 or 1343;'';

(2) in subsection (c)(3)—

(A) in subparagraph (A), by striking ''(a)(4) or (a)(7)'' and inserting ''(a)(4), (a)(7), or (a)(8)''; and

(B) in subparagraph (B), by striking ''(a)(4), or (a)(7)'' and inserting ''(a)(4), (a)(7), or (a)(8)'';

(3) in subsection (e)—

(A) in paragraph (11), by striking ''and'' at the end;

(B) in paragraph (12), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(13) the term 'traffic', except as provided in subsection (a)(6), means transfer, or otherwise dispose of, to another as consideration for the receipt of, or as consideration for a promise or agreement to pay, anything of pecuniary value.''; and

(4) in subsection (g), in the first sentence, by inserting '', except for a violation of subsection (a)(8),'' after ''of this section''.

SA 2714. Mr. BARRASSO submitted an amendment intended to be proposed by him to the bill S. 209, to amend the Indian Tribal Energy Development and Self-Determination Act of 2005, and for other purposes; which was ordered to lie on the table; as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Indian Tribal Energy Development and Self-Determination Act Amendments of 2015''.

SEC. 2. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

Sec. 1. Short title.
Sec. 2. Table of contents.
TITLE I—INDIAN TRIBAL ENERGY DEVELOPMENT AND SELF-DETERMINATION ACT AMENDMENTS
Sec. 101. Indian tribal energy resource development.
Sec. 102. Indian tribal energy resource regulation.
Sec. 103. Tribal energy resource agreements.
Sec. 104. Technical assistance for Indian tribal governments.
Sec. 105. Conforming amendments.
Sec. 106. Report.

TITLE II—MISCELLANEOUS AMENDMENTS

Sec. 201. Issuance of preliminary permits or licenses.
Sec. 202. Tribal biomass demonstration project.
Sec. 203. Weatherization program.
Sec. 204. Appraisals.
Sec. 205. Leases of restricted lands for Navajo Nation.
Sec. 206. Extension of tribal lease period for the Crow Tribe of Montana.
Sec. 207. Trust status of lease payments.

TITLE I—INDIAN TRIBAL ENERGY DEVELOPMENT AND SELF-DETERMINATION ACT AMENDMENTS

SEC. 101. INDIAN TRIBAL ENERGY RESOURCE DEVELOPMENT.

(a) IN GENERAL.—Section 2602(a) of the Energy Policy Act of 1992 (25 U.S.C. 3502(a)) is amended—

(1) in paragraph (2)—

(A) in subparagraph (C), by striking ''and'' after the semicolon;

(B) in subparagraph (D), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(E) consult with each applicable Indian tribe before adopting or approving a well spacing program or plan applicable to the energy resources of that Indian tribe or the members of that Indian tribe.''; and

(2) by adding at the end the following:

''(4) PLANNING.—

''(A) IN GENERAL.—In carrying out the program established by paragraph (1), the Secretary shall provide technical assistance to interested Indian tribes to develop energy plans, including—

''(i) plans for electrification;

''(ii) plans for oil and gas permitting, renewable energy permitting, energy efficiency, electricity generation, transmission planning, water planning, and other planning relating to energy issues;

''(iii) plans for the development of energy resources and to ensure the protection of natural, historic, and cultural resources; and

''(iv) any other plans that would assist an Indian tribe in the development or use of energy resources.

''(B) COOPERATION.—In establishing the program under paragraph (1), the Secretary shall work in cooperation with the Office of Indian Energy Policy and Programs of the Department of Energy.''.

(b) DEPARTMENT OF ENERGY INDIAN ENERGY EDUCATION PLANNING AND MANAGEMENT ASSISTANCE PROGRAM.—Section 2602(b)(2) of the Energy Policy Act of 1992 (25 U.S.C. 3502(b)(2)) is amended—

(1) in the matter preceding subparagraph (A), by inserting '', intertribal organization,'' after ''Indian tribe'';

(2) by redesignating subparagraphs (C) and (D) as subparagraphs (D) and (E), respectively; and

(3) by inserting after subparagraph (B) the following:

''(C) activities to increase the capacity of Indian tribes to manage energy development and energy efficiency programs;''.

(c) DEPARTMENT OF ENERGY LOAN GUARANTEE PROGRAM.—Section 2602(c) of the Energy Policy Act of 1992 (25 U.S.C. 3502(c)) is amended—

(1) in paragraph (1), by inserting ''or a tribal energy development organization'' after ''Indian tribe'';

(2) in paragraph (3)—

(A) in the matter preceding subparagraph (A), by striking ''guarantee'' and inserting ''guaranteed'';

(B) in subparagraph (A), by striking ''or'';

(C) in subparagraph (B), by striking the period at the end and inserting ''; or''; and

(D) by adding at the end the following:

''(C) a tribal energy development organization, from funds of the tribal energy development organization.''; and

(3) in paragraph (5), by striking ''The Secretary of Energy may'' and inserting ''Not later than 1 year after the date of enactment of the Indian Tribal Energy Development and Self-Determination Act Amendments of 2015, the Secretary of Energy shall''.

SEC. 102. INDIAN TRIBAL ENERGY RESOURCE REGULATION.

Section 2603(c) of the Energy Policy Act of 1992 (25 U.S.C. 3503(c)) is amended—

(1) in paragraph (1), by striking ''on the request of an Indian tribe, the Indian tribe'' and inserting ''on the request of an Indian tribe or a tribal energy development organization, the Indian tribe or tribal energy development organization''; and

(2) in paragraph (2)(B), by inserting ''or tribal energy development organization'' after ''Indian tribe''.

SEC. 103. TRIBAL ENERGY RESOURCE AGREEMENTS.

(a) AMENDMENT.—Section 2604 of the Energy Policy Act of 1992 (25 U.S.C. 3504) is amended—

(1) in subsection (a)—

(A) in paragraph (1)—

(i) in subparagraph (A), by striking ''or'' after the semicolon at the end;

(ii) in subparagraph (B)—

(I) by striking clause (i) and inserting the following:

''(i) an electric production, generation, transmission, or distribution facility (including a facility that produces electricity from renewable energy resources) located on tribal land; or''; and

(II) in clause (ii)—

(aa) by inserting '', at least a portion of which have been'' after ''energy resources'';

(bb) by inserting ''or produced from'' after ''developed on''; and

(cc) by striking ''and'' after the semicolon at the end and inserting ''or''; and

(iii) by adding at the end the following:

''(C) pooling, unitization, or communitization of the energy mineral resources of the Indian tribe located on tribal land with any other energy mineral resource (including energy mineral resources owned by the Indian tribe or an individual Indian in fee, trust, or restricted status or by any other persons or entities) if the owner, or, if appropriate, lessee, of the resources has consented or consents to the pooling, unitization, or communitization of the other resources under any lease or agreement; and''; and

(B) by striking paragraph (2) and inserting the following:

''(2) a lease or business agreement described in paragraph (1) shall not require review by, or the approval of, the Secretary under section 2103 of the Revised Statutes (25 U.S.C. 81), or any other provision of law (including regulations), if the lease or business agreement—

''(A) was executed—

''(i) in accordance with the requirements of a tribal energy resource agreement in effect under subsection (e) (including the periodic review and evaluation of the activities of the Indian tribe under the agreement, to be conducted pursuant to subparagraphs (D) and (E) of subsection (e)(2)); or

''(ii) by the Indian tribe and a tribal energy development organization for which the Indian tribe has obtained a certification pursuant to subsection (h); and

''(B) has a term that does not exceed—

''(i) 30 years; or

''(ii) in the case of a lease for the production of oil resources, gas resources, or both, 10 years and as long thereafter as oil or gas is produced in paying quantities.'';

(2) by striking subsection (b) and inserting the following:

''(b) RIGHTS-OF-WAY.—An Indian tribe may grant a right-of-way over tribal land without review or approval by the Secretary if the right-of-way—

''(1) serves—

''(A) an electric production, generation, transmission, or distribution facility (including a facility that produces electricity from renewable energy resources) located on tribal land;

''(B) a facility located on tribal land that extracts, produces, processes, or refines energy resources; or

''(C) the purposes, or facilitates in carrying out the purposes, of any lease or agreement entered into for energy resource development on tribal land;

''(2) was executed—

''(A) in accordance with the requirements of a tribal energy resource agreement in effect under subsection (e) (including the periodic review and evaluation of the activities of the Indian tribe under the agreement, to be conducted pursuant to subparagraphs (D) and (E) of subsection (e)(2)); or

''(B) by the Indian tribe and a tribal energy development organization for which the Indian tribe has obtained a certification pursuant to subsection (h); and

''(3) has a term that does not exceed 30 years.'';

(3) by striking subsection (d) and inserting the following:

''(d) VALIDITY.—No lease or business agreement entered into, or right-of-way granted, pursuant to this section shall be valid unless the lease, business agreement, or right-of-way is authorized by subsection (a) or (b).'';

(4) in subsection (e)—

(A) by striking paragraph (1) and inserting the following:

''(1) IN GENERAL.—

''(A) AUTHORIZATION.—On or after the date of enactment of the Indian Tribal Energy Development and Self-Determination Act Amendments of 2015, a qualified Indian tribe may submit to the Secretary a tribal energy resource agreement governing leases, business agreements, and rights-of-way under this section.

''(B) NOTICE OF COMPLETE PROPOSED AGREEMENT.—Not later than 60 days after the date on which the tribal energy resource agreement is submitted under subparagraph (A), the Secretary shall—

''(i) notify the Indian tribe as to whether the agreement is complete or incomplete;

''(ii) if the agreement is incomplete, notify the Indian tribe of what information or documentation is needed to complete the submission; and

''(iii) identify and notify the Indian tribe of the financial assistance, if any, to be provided by the Secretary to the Indian tribe to assist in the implementation of the tribal energy resource agreement, including the environmental review of individual projects.

''(C) EFFECT.—Nothing in this paragraph precludes the Secretary from providing any financial assistance at any time to the Indian tribe to assist in the implementation of the tribal energy resource agreement.'';

(B) in paragraph (2)—

(i) by striking ''(2)(A)'' and all that follows through the end of subparagraph (A) and inserting the following:

''(2) PROCEDURE.—

''(A) EFFECTIVE DATE.—

''(i) IN GENERAL.—On the date that is 271 days after the date on which the Secretary receives a tribal energy resource agreement from a qualified Indian tribe under paragraph (1), the tribal energy resource agreement shall take effect, unless the Secretary disapproves the tribal energy resource agreement under subparagraph (B).

''(ii) REVISED TRIBAL ENERGY RESOURCE AGREEMENT.—On the date that is 91 days after the date on which the Secretary receives a revised tribal energy resource agreement from a qualified Indian tribe under paragraph (4)(B), the revised tribal energy resource agreement shall take effect, unless the Secretary disapproves the revised tribal energy resource agreement under subparagraph (B).'';

(ii) in subparagraph (B)—

(I) by striking ''(B)'' and all that follows through clause (ii) and inserting the following:

''(B) DISAPPROVAL.—The Secretary shall disapprove a tribal energy resource agreement submitted pursuant to paragraph (1) or (4)(B) only if—

''(i) a provision of the tribal energy resource agreement violates applicable Federal law (including regulations) or a treaty applicable to the Indian tribe;

''(ii) the tribal energy resource agreement does not include 1 or more provisions required under subparagraph (D); or''; and

(II) in clause (iii)—

(aa) in the matter preceding subclause (I), by striking ''includes'' and all that follows through ''section—'' and inserting ''does not include provisions that, with respect to any lease, business agreement, or right-of-way to which the tribal energy resource agreement applies—'';

(bb) by striking subclauses (I), (II), (V), (VIII), and (XV);

(cc) by redesignating clauses (III), (IV), (VI), (VII), (IX) through (XIV), and (XVI) as clauses (I), (II), (III), (IV), (V) through (X), and (XI), respectively;

(dd) in item (bb) of subclause (XI) (as redesignated by item (cc))—

(AA) by striking ''or tribal''; and

(BB) by striking the period at the end and inserting a semicolon; and

(ee) by adding at the end the following:

''(XII) include a certification by the Indian tribe that the Indian tribe has—

''(aa) carried out a contract or compact under title I or IV of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450 et seq.) for a period of not less than 3 consecutive years ending on the date on which the Indian tribe submits the application without material audit exception (or without any material audit exceptions that were not corrected within the 3-year period) relating to the management of tribal land or natural resources; or

''(bb) substantial experience in the administration, review, or evaluation of energy resource leases or agreements or has otherwise substantially participated in the administration, management, or development of energy resources located on the tribal land of the Indian tribe; and

''(XIII) at the option of the Indian tribe, identify which functions, if any, authorizing any operational or development activities pursuant to a lease, right-of-way, or business agreement approved by the Indian tribe, that the Indian tribe intends to conduct.'';

(iii) in subparagraph (C)—

(I) by striking clauses (i) and (ii);

(II) by redesignating clauses (iii) through (v) as clauses (ii) through (iv), respectively; and

(III) by inserting before clause (ii) (as redesignated by subclause (II)) the following:

''(i) a process for ensuring that—

''(I) the public is informed of, and has reasonable opportunity to comment on, any significant environmental impacts of the proposed action; and

''(II) the Indian tribe provides responses to relevant and substantive public comments on any impacts described in subclause (I) before the Indian tribe approves the lease, business agreement, or right-of-way.'';

(iv) in subparagraph (D)(ii), by striking ''subparagraph (B)(iii)(XVI)'' and inserting ''subparagraph (B)(iv)(XI)''; and

(v) by adding at the end the following:

''(F) EFFECTIVE PERIOD.—A tribal energy resource agreement that takes effect pursuant to this subsection shall remain in effect to the extent any provision of the tribal energy resource agreement is consistent with applicable Federal law (including regulations), unless the tribal energy resource agreement is—

''(i) rescinded by the Secretary pursuant to paragraph (7)(D)(iii)(II); or

''(ii) voluntarily rescinded by the Indian tribe pursuant to the regulations promulgated under paragraph (8)(B) (or successor regulations).'';

(C) in paragraph (4), by striking ''date of disapproval'' and all that follows through the end of subparagraph (C) and inserting the following: ''date of disapproval, provide the Indian tribe with—

''(A) a detailed, written explanation of—

''(i) each reason for the disapproval; and

''(ii) the revisions or changes to the tribal energy resource agreement necessary to address each reason; and

''(B) an opportunity to revise and resubmit the tribal energy resource agreement.'';

(D) in paragraph (6)—

(i) in subparagraph (B)—

(I) by striking ''(B) Subject to'' and inserting the following:

''(B) Subject only to''; and

(II) by striking ''subparagraph (D)'' and inserting ''subparagraphs (C) and (D)'';

(ii) in subparagraph (C), in the matter preceding clause (i), by inserting ''to perform the obligations of the Secretary under this section and'' before ''to ensure''; and

(iii) in subparagraph (D), by adding at the end the following:

''(iii) Nothing in this section absolves, limits, or otherwise affects the liability, if any, of the United States for any—

''(I) term of any lease, business agreement, or right-of-way under this section that is not a negotiated term; or

''(II) losses that are not the result of a negotiated term, including losses resulting from the failure of the Secretary to perform an obligation of the Secretary under this section.'';

(E) in paragraph (7)—

(i) in subparagraph (A), by striking ''has demonstrated'' and inserting ''the Secretary determines has demonstrated with substantial evidence'';

(ii) in subparagraph (B), by striking ''any tribal remedy'' and inserting ''all remedies (if any) provided under the laws of the Indian tribe'';

(iii) in subparagraph (D)—

(I) in clause (i), by striking ''determine'' and all that follows through the end of the clause and inserting the following: ''determine—

''(I) whether the petitioner is an interested party; and

''(II) if the petitioner is an interested party, whether the Indian tribe is not in compliance with the tribal energy resource agreement as alleged in the petition.'';

(II) in clause (ii), by striking ''determination'' and inserting ''determinations''; and

(III) in clause (iii), in the matter preceding subclause (I) by striking ''agreement'' the first place it appears and all that follows through '', including'' and inserting ''agreement pursuant to clause (i), the Secretary shall only take such action as the Secretary determines necessary to address the claims of noncompliance made in the petition, including'';

(iv) in subparagraph (E)(i), by striking ''the manner in which'' and inserting '', with respect to each claim made in the petition, how''; and

(v) by adding at the end the following:

''(G) Notwithstanding any other provision of this paragraph, the Secretary shall dismiss any petition from an interested party that has agreed with the Indian tribe to a resolution of the claims presented in the petition of that party.'';

(F) in paragraph (8)—

(i) by striking subparagraph (A);

(ii) by redesignating subparagraphs (B) through (D) as subparagraphs (A) through (C), respectively; and

(iii) in subparagraph (A) (as redesignated by clause (ii))—

(I) in clause (i), by striking ''and'' at the end;

(II) in clause (ii), by adding ''and'' after the semicolon; and

(III) by adding at the end the following:

''(iii) amend an approved tribal energy resource agreement to assume authority for approving leases, business agreements, or rights-of-way for development of another energy resource that is not included in an approved tribal energy resource agreement without being required to apply for a new tribal energy resource agreement;'' and

(G) by adding at the end the following:

''(9) EFFECT.—Nothing in this section authorizes the Secretary to deny a tribal energy resource agreement or any amendment to a tribal energy resource agreement, or to limit the effect or implementation of this section, due to lack of promulgated regulations.'';

(5) by redesignating subsection (g) as subsection (j); and

(6) by inserting after subsection (f) the following:

''(g) FINANCIAL ASSISTANCE IN LIEU OF ACTIVITIES BY THE SECRETARY.—

''(1) IN GENERAL.—Any amounts that the Secretary would otherwise expend to operate or carry out any program, function, service, or activity (or any portion of a program, function, service, or activity) of the Department that, as a result of an Indian tribe carrying out activities under a tribal energy resource agreement, the Secretary does not expend, the Secretary shall, at the request of the Indian tribe, make available to the Indian tribe in accordance with this subsection.

''(2) ANNUAL FUNDING AGREEMENTS.—The Secretary shall make the amounts described in paragraph (1) available to an Indian tribe through an annual written funding agreement that is negotiated and entered into with the Indian tribe that is separate from the tribal energy resource agreement.

''(3) EFFECT OF APPROPRIATIONS.—Notwithstanding paragraph (1)—

''(A) the provision of amounts to an Indian tribe under this subsection is subject to the availability of appropriations; and

''(B) the Secretary shall not be required to reduce amounts for programs, functions, services, or activities that serve any other Indian tribe to make amounts available to an Indian tribe under this subsection.

''(4) DETERMINATION.—

''(A) IN GENERAL.—The Secretary shall calculate the amounts under paragraph (1) in accordance with the regulations adopted under section 103(b) of the Indian Tribal Energy Development and Self-Determination Act Amendments of 2015.

''(B) APPLICABILITY.—The effective date or implementation of a tribal energy resource agreement under this section shall not be delayed or otherwise affected by—

''(i) a delay in the promulgation of regulations under section 103(b) of the Indian Tribal Energy Development and Self-Determination Act Amendments of 2015;

''(ii) the period of time needed by the Secretary to make the calculation required under paragraph (1); or

''(iii) the adoption of a funding agreement under paragraph (2).

''(h) CERTIFICATION OF TRIBAL ENERGY DEVELOPMENT ORGANIZATION.—

''(1) IN GENERAL.—Not later than 90 days after the date on which an Indian tribe submits an application for certification of a tribal energy development organization in accordance with regulations promulgated under section 103(b) of the Indian Tribal Energy Development and Self-Determination Act Amendments of 2015, the Secretary shall approve or disapprove the application.

''(2) REQUIREMENTS.—The Secretary shall approve an application for certification if—

''(A)(i) the Indian tribe has carried out a contract or compact under title I or IV of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450 et seq.); and

''(ii) for a period of not less than 3 consecutive years ending on the date on which the Indian tribe submits the application, the contract or compact—

''(I) has been carried out by the Indian tribe without material audit exceptions (or without any material audit exceptions that were not corrected within the 3-year period); and

''(II) has included programs or activities relating to the management of tribal land; and

''(B)(i) the tribal energy development organization is organized under the laws of the Indian tribe;

''(ii)(I) the majority of the interest in the tribal energy development organization is owned and controlled by the Indian tribe (or the Indian tribe and 1 or more other Indian tribes) the tribal land of which is being developed; and

''(II) the organizing document of the tribal energy development organization requires that the Indian tribe with jurisdiction over the land maintain at all times the controlling interest in the tribal energy development organization;

''(iii) the organizing document of the tribal energy development organization requires that the Indian tribe (or the Indian tribe and 1 or more other Indian tribes) the tribal land of which is being developed own and control at all times a majority of the interest in the tribal energy development organization; and

''(iv) the organizing document of the tribal energy development organization includes a statement that the organization shall be subject to the jurisdiction, laws, and authority of the Indian tribe.

''(3) ACTION BY SECRETARY.—If the Secretary approves an application for certification pursuant to paragraph (2), the Secretary shall, not more than 10 days after making the determination—

''(A) issue a certification stating that—

''(i) the tribal energy development organization is organized under the laws of the Indian tribe and subject to the jurisdiction, laws, and authority of the Indian tribe;

''(ii) the majority of the interest in the tribal energy development organization is owned and controlled by the Indian tribe (or the Indian tribe and 1 or more other Indian tribes) the tribal land of which is being developed;

''(iii) the organizing document of the tribal energy development organization requires that the Indian tribe with jurisdiction over the land maintain at all times the controlling interest in the tribal energy development organization;

''(iv) the organizing document of the tribal energy development organization requires that the Indian tribe (or the Indian tribe and 1 or more other Indian tribes the tribal land of which is being developed) own and control at all times a majority of the interest in the tribal energy development organization; and

''(v) the certification is issued pursuant this subsection;

''(B) deliver a copy of the certification to the Indian tribe; and

''(C) publish the certification in the Federal Register.

''(i) SOVEREIGN IMMUNITY.—Nothing in this section waives the sovereign immunity of an Indian tribe.''.

(b) REGULATIONS.—Not later than 1 year after the date of enactment of the Indian Tribal Energy Development and Self-Determination Act Amendments of 2015, the Secretary shall promulgate or update any regulations that are necessary to implement this section, including provisions to implement—

(1) section 2604(e)(8) of the Energy Policy Act of 1992 (25 U.S.C. 3504(e)(8)), including the process to be followed by an Indian tribe amending an existing tribal energy resource agreement to assume authority for approving leases, business agreements, or rights-of-way for development of an energy resource that is not included in the tribal energy resource agreement;

(2) section 2604(g) of the Energy Policy Act of 1992 (25 U.S.C. 3504(g)) including the manner in which the Secretary, at the request of an Indian tribe, shall—

(A) identify the programs, functions, services, and activities (or any portions of programs, functions, services, or activities) that the Secretary will not have to operate or carry out as a result of the Indian tribe carrying out activities under a tribal energy resource agreement;

(B) identify the amounts that the Secretary would have otherwise expended to operate or carry out each program, function, service, and activity (or any portion of a program, function, service, or activity) identified pursuant to subparagraph (A); and

(C) provide to the Indian tribe a list of the programs, functions, services, and activities (or any portions of programs, functions, services, or activities) identified pursuant subparagraph (A) and the amounts associated with each program, function, service, and activity (or any portion of a program, function, service, or activity) identified pursuant to subparagraph (B); and

(3) section 2604(h) of the Energy Policy Act of 1992 (25 U.S.C. 3504(h)), including the process to be followed by, and any applicable criteria and documentation required for, an Indian tribe to request and obtain the certification described in that section.

SEC. 104. TECHNICAL ASSISTANCE FOR INDIAN TRIBAL GOVERNMENTS.

Section 2602(b) of the Energy Policy Act of 1992 (25 U.S.C. 3502(b)) is amended—

(1) by redesignating paragraphs (3) through (6) as paragraphs (4) through (7), respectively; and

(2) by inserting after paragraph (2) the following:

''(3) TECHNICAL AND SCIENTIFIC RESOURCES.—In addition to providing grants to Indian tribes under this subsection, the Secretary shall collaborate with the Directors of the National Laboratories in making the full array of technical and scientific resources of the Department of Energy available for tribal energy activities and projects.''.

SEC. 105. CONFORMING AMENDMENTS.

(a) DEFINITION OF TRIBAL ENERGY DEVELOPMENT ORGANIZATION.—Section 2601 of the Energy Policy Act of 1992 (25 U.S.C. 3501) is amended—

(1) by redesignating paragraphs (9) through (12) as paragraphs (10) through (13), respectively;

(2) by inserting after paragraph (8) the following:

''(9) The term 'qualified Indian tribe' means an Indian tribe that has—

''(A) carried out a contract or compact under title I or IV of the Indian Self Determination and Education Assistance Act (25 U.S.C. 450 et seq.) for a period of not less than 3 consecutive years ending on the date on which the Indian tribe submits the application without material audit exception (or without any material audit exceptions that were not corrected within the 3-year period) relating to the management of tribal land or natural resources; or

''(B) substantial experience in the administration, review, or evaluation of energy resource leases or agreements or has otherwise substantially participated in the administration, management, or development of energy resources located on the tribal land of the Indian tribe.''; and

(3) by striking paragraph (12) (as redesignated by paragraph (1)) and inserting the following:

''(12) The term 'tribal energy development organization' means—

''(A) any enterprise, partnership, consortium, corporation, or other type of business organization that is engaged in the development of energy resources and is wholly owned by an Indian tribe (including an organization incorporated pursuant to section 17 of the Indian Reorganization Act of 1934 (25 U.S.C. 477) or section 3 of the Act of June 26, 1936 (25 U.S.C. 503) (commonly known as the 'Oklahoma Indian Welfare Act')); and

''(B) any organization of 2 or more entities, at least 1 of which is an Indian tribe, that has the written consent of the governing bodies of all Indian tribes participating in the organization to apply for a grant, loan, or other assistance under section 2602 or to enter into a lease or business agreement with, or acquire a right-of-way from, an Indian tribe pursuant to subsection (a)(2)(A)(ii) or (b)(2)(B) of section 2604.''.

(b) INDIAN TRIBAL ENERGY RESOURCE DEVELOPMENT.—Section 2602 of the Energy Policy Act of 1992 (25 U.S.C. 3502) is amended—

(1) in subsection (a)—

(A) in paragraph (1), by striking ''tribal energy resource development organizations'' and inserting ''tribal energy development organizations''; and

(B) in paragraph (2), by striking ''tribal energy resource development organizations'' each place it appears and inserting ''tribal energy development organizations''; and

(2) in subsection (b)(2), by striking ''tribal energy resource development organization'' and inserting ''tribal energy development organization''.

(c) WIND AND HYDROPOWER FEASIBILITY STUDY.—Section 2606(c)(3) of the Energy Policy Act of 1992 (25 U.S.C. 3506(c)(3)) is amended by striking ''energy resource development'' and inserting ''energy development''.

(d) CONFORMING AMENDMENTS.—Section 2604(e) of the Energy Policy Act of 1992 (25 U.S.C. 3504(e)) is amended—

(1) in paragraph (3)—

(A) by striking ''(3) The Secretary'' and inserting the following:

''(3) NOTICE AND COMMENT; SECRETARIAL REVIEW.—The Secretary''; and

(B) by striking ''for approval'';

(2) in paragraph (4), by striking ''(4) If the Secretary'' and inserting the following:

''(4) ACTION IN CASE OF DISAPPROVAL.—If the Secretary'';

(3) in paragraph (5)—

(A) by striking ''(5) If an Indian tribe'' and inserting the following:

''(5) PROVISION OF DOCUMENTS TO SECRETARY.—If an Indian tribe''; and

(B) in the matter preceding subparagraph (A), by striking ''approved'' and inserting ''in effect'';

(4) in paragraph (6)—

(A) by striking ''(6)(A) In carrying out'' and inserting the following:

''(6) SECRETARIAL OBLIGATIONS AND EFFECT OF SECTION.—

''(A) In carrying out'';

(B) in subparagraph (A), by indenting clauses (i) and (ii) appropriately;

(C) in subparagraph (B), by striking ''approved'' and inserting ''in effect''; and

(D) in subparagraph (D)—

(i) in clause (i), by striking ''an approved tribal energy resource agreement'' and inserting ''a tribal energy resource agreement in effect under this section''; and

(ii) in clause (ii), by striking ''approved by the Secretary'' and inserting ''in effect''; and

(5) in paragraph (7)—

(A) by striking ''(7)(A) In this paragraph'' and inserting the following:

''(7) PETITIONS BY INTERESTED PARTIES.—

''(A) In this paragraph'';

(B) in subparagraph (A), by striking ''approved by the Secretary'' and inserting ''in effect'';

(C) in subparagraph (B), by striking ''approved by the Secretary'' and inserting ''in effect''; and

(D) in subparagraph (D)(iii)—

(i) in subclause (I), by striking ''approved''; and

(ii) in subclause (II)—

(I) by striking ''approval of'' in the first place it appears; and

(II) by striking ''subsection (a) or (b)'' and inserting ''subsection (a)(2)(A)(i) or (b)(2)(A)''.

SEC. 106. REPORT.

(a) IN GENERAL.—Not later than 18 months after the date of enactment of this Act, the Secretary of the Interior shall submit to the Committee on Indian Affairs of the Senate and the Committee on Natural Resources of the House of Representatives a report that details with respect to activities for energy development on Indian land, how the Department of the Interior—

(1) processes and completes the reviews of energy-related documents in a timely and transparent manner;

(2) monitors the timeliness of agency review for all energy-related documents;

(3) maintains databases to track and monitor the review and approval process for energy-related documents associated with conventional and renewable Indian energy resources that require Secretarial approval prior to development, including—

(A) any seismic exploration permits;

(B) permission to survey;

(C) archeological and cultural surveys;

(D) access permits;

(E) environmental assessments;

(F) oil and gas leases;

(G) surface leases;

(H) rights-of-way agreements; and

(I) communitization agreements;

(4) identifies in the databases—

(A) the date lease applications and permits are received by the agency;

(B) the status of the review;

(C) the date the application or permit is considered complete and ready for review;

(D) the date of approval; and

(E) the start and end dates for any significant delays in the review process;

(5) tracks in the databases, for all energy-related leases, agreements, applications, and permits that involve multiple agency review—

(A) the dates documents are transferred between agencies;

(B) the status of the review;

(C) the date the required reviews are completed; and

(D) the date interim or final decisions are issued.

(b) INCLUSIONS.—The report under subsection (a) shall include—

(1) a description of any intermediate and final deadlines for agency action on any Secretarial review and approval required for Indian conventional and renewable energy exploration and development activities;

(2) a description of the existing geographic database established by the Bureau of Indian Affairs, explaining—

(A) how the database identifies—

(i) the location and ownership of all Indian oil and gas resources held in trust;

(ii) resources available for lease; and

(iii) the location of—

(I) any lease of land held in trust or restricted fee on behalf of any Indian tribe or individual Indian; and

(II) any rights-of-way on that land in effect;

(B) how the information from the database is made available to—

(i) the officials of the Bureau of Indian Affairs with responsibility over the management and development of Indian resources; and

(ii) resource owners; and

(C) any barriers to identifying the information described in subparagraphs (A) and (B) or any deficiencies in that information; and

(3) an evaluation of—

(A) the ability of each applicable agency to track and monitor the review and approval process of the agency for Indian energy development; and

(B) the extent to which each applicable agency complies with any intermediate and final deadlines.

TITLE II—MISCELLANEOUS AMENDMENTS

SEC. 201. ISSUANCE OF PRELIMINARY PERMITS OR LICENSES.

(a) IN GENERAL.—Section 7(a) of the Federal Power Act (16 U.S.C. 800(a)) is amended by striking ''States and municipalities'' and inserting ''States, Indian tribes, and municipalities''.

(b) APPLICABILITY.—The amendment made by subsection (a) shall not affect—

(1) any preliminary permit or original license issued before the date of enactment of the Indian Tribal Energy Development and Self-Determination Act Amendments of 2015; or

(2) an application for an original license, if the Commission has issued a notice accepting that application for filing pursuant to section 4.32(d) of title 18, Code of Federal Regulations (or successor regulations), before the date of enactment of the Indian Tribal Energy Development and Self-Determination Act Amendments of 2015.

(c) DEFINITION OF INDIAN TRIBE.—For purposes of section 7(a) of the Federal Power Act (16 U.S.C. 800(a)) (as amended by subsection (a)), the term ''Indian tribe'' has the meaning given the term in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SEC. 202. TRIBAL BIOMASS DEMONSTRATION PROJECT.

(a) PURPOSE.—The purpose of this section is to establish a biomass demonstration project for federally recognized Indian tribes and Alaska Native corporations to promote biomass energy production.

(b) TRIBAL BIOMASS DEMONSTRATION PROJECT.—The Tribal Forest Protection Act of 2004 (Public Law 108–278; 118 Stat. 868) is amended—

(1) in section 2(a), by striking ''In this section'' and inserting ''In this Act''; and

(2) by adding at the end the following:

''SEC. 3. TRIBAL BIOMASS DEMONSTRATION PROJECT.

''(a) STEWARDSHIP CONTRACTS OR SIMILAR AGREEMENTS.—For each of fiscal years 2016 through 2020, the Secretary shall enter into stewardship contracts or similar agreements (excluding direct service contracts) with Indian tribes to carry out demonstration projects to promote biomass energy production (including biofuel, heat, and electricity generation) on Indian forest land and in nearby communities by providing reliable supplies of woody biomass from Federal land.

''(b) DEMONSTRATION PROJECTS.—In each fiscal year for which projects are authorized, at least 4 new demonstration projects that meet the eligibility criteria described in subsection (c) shall be carried out under contracts or agreements described in subsection (a).

''(c) ELIGIBILITY CRITERIA.—To be eligible to enter into a contract or agreement under this section, an Indian tribe shall submit to the Secretary an application—

''(1) containing such information as the Secretary may require; and

''(2) that includes a description of—

''(A) the Indian forest land or rangeland under the jurisdiction of the Indian tribe; and

''(B) the demonstration project proposed to be carried out by the Indian tribe.

''(d) SELECTION.—In evaluating the applications submitted under subsection (c), the Secretary shall—

''(1) take into consideration—

''(A) the factors set forth in paragraphs (1) and (2) of section 2(e); and

''(B) whether a proposed project would—

''(i) increase the availability or reliability of local or regional energy;

''(ii) enhance the economic development of the Indian tribe;

''(iii) result in or improve the connection of electric power transmission facilities serving the Indian tribe with other electric transmission facilities;

''(iv) improve the forest health or watersheds of Federal land or Indian forest land or rangeland;

''(v) demonstrate new investments in infrastructure; or

''(vi) otherwise promote the use of woody biomass; and

''(2) exclude from consideration any merchantable logs that have been identified by the Secretary for commercial sale.

''(e) IMPLEMENTATION.—The Secretary shall—

''(1) ensure that the criteria described in subsection (c) are publicly available by not later than 120 days after the date of enactment of this section; and

''(2) to the maximum extent practicable, consult with Indian tribes and appropriate intertribal organizations likely to be affected in developing the application and otherwise carrying out this section.

''(f) REPORT.—Not later than September 20, 2018, the Secretary shall submit to Congress a report that describes, with respect to the reporting period—

''(1) each individual tribal application received under this section; and

''(2) each contract and agreement entered into pursuant to this section.

''(g) INCORPORATION OF MANAGEMENT PLANS.—In carrying out a contract or agreement under this section, on receipt of a request from an Indian tribe, the Secretary shall incorporate into the contract or agreement, to the maximum extent practicable, management plans (including forest management and integrated resource management plans) in effect on the Indian forest land or rangeland of the respective Indian tribe.

''(h) TERM.—A contract or agreement entered into under this section—

''(1) shall be for a term of not more than 20 years; and

''(2) may be renewed in accordance with this section for not more than an additional 10 years.''.

(c) ALASKA NATIVE BIOMASS DEMONSTRATION PROJECT.—

(1) DEFINITIONS.—In this subsection:

(A) FEDERAL LAND.—The term ''Federal land'' means—

(i) land of the National Forest System (as defined in section 11(a) of the Forest and Rangeland Renewable Resources Planning Act of 1974 (16 U.S.C. 1609(a)) administered by the Secretary of Agriculture, acting through the Chief of the Forest Service; and

(ii) public lands (as defined in section 103 of the Federal Land Policy Management Act of 1976 (43 U.S.C. 1702)), the surface of which is administered by the Secretary of the Interior, acting through the Director of the Bureau of Land Management.

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

(C) SECRETARY.—The term ''Secretary'' means—

(i) the Secretary of Agriculture, with respect to land under the jurisdiction of the Forest Service; and

(ii) the Secretary of the Interior, with respect to land under the jurisdiction of the Bureau of Land Management.

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

(2) AGREEMENTS.—For each of fiscal years 2016 through 2020, the Secretary shall enter into an agreement or contract with an Indian tribe or a tribal organization to carry out a demonstration project to promote biomass energy production (including biofuel, heat, and electricity generation) by providing reliable supplies of woody biomass from Federal land.

(3) DEMONSTRATION PROJECTS.—In each fiscal year for which projects are authorized, at least 1 new demonstration project that meets the eligibility criteria described in paragraph (4) shall be carried out under contracts or agreements described in paragraph (2).

(4) ELIGIBILITY CRITERIA.—To be eligible to enter into a contract or agreement under this subsection, an Indian tribe or tribal organization shall submit to the Secretary an application—

(A) containing such information as the Secretary may require; and

(B) that includes a description of the demonstration project proposed to be carried out by the Indian tribe or tribal organization.

(5) SELECTION.—In evaluating the applications submitted under paragraph (4), the Secretary shall—

(A) take into consideration whether a proposed project would—

(i) increase the availability or reliability of local or regional energy;

(ii) enhance the economic development of the Indian tribe;

(iii) result in or improve the connection of electric power transmission facilities serving the Indian tribe with other electric transmission facilities;

(iv) improve the forest health or watersheds of Federal land or non-Federal land;

(v) demonstrate new investments in infrastructure; or

(vi) otherwise promote the use of woody biomass; and

(B) exclude from consideration any merchantable logs that have been identified by the Secretary for commercial sale.

(6) IMPLEMENTATION.—The Secretary shall—

(A) ensure that the criteria described in paragraph (4) are publicly available by not later than 120 days after the date of enactment of this subsection; and

(B) to the maximum extent practicable, consult with Indian tribes and appropriate tribal organizations likely to be affected in developing the application and otherwise carrying out this subsection.

(7) REPORT.—Not later than September 20, 2018, the Secretary shall submit to Congress a report that describes, with respect to the reporting period—

(A) each individual application received under this subsection; and

(B) each contract and agreement entered into pursuant to this subsection.

(8) TERM.—A contract or agreement entered into under this subsection—

(A) shall be for a term of not more than 20 years; and

(B) may be renewed in accordance with this subsection for not more than an additional 10 years.

SEC. 203. WEATHERIZATION PROGRAM.

Section 413(d) of the Energy Conservation and Production Act (42 U.S.C. 6863(d)) is amended—

(1) by striking paragraph (1) and inserting the following:

''(1) RESERVATION OF AMOUNTS.—

''(A) IN GENERAL.—Subject to subparagraph (B) and notwithstanding any other provision of this part, the Secretary shall reserve from amounts that would otherwise be allocated to a State under this part not less than 100 percent, but not more than 150 percent, of an amount which bears the same proportion to the allocation of that State for the applicable fiscal year as the population of all low-income members of an Indian tribe in that State bears to the population of all low-income individuals in that State.

''(B) RESTRICTIONS.—Subparagraph (A) shall apply only if—

''(i) the tribal organization serving the low-income members of the applicable Indian tribe requests that the Secretary make a grant directly; and

''(ii) the Secretary determines that the low-income members of the applicable Indian tribe would be equally or better served by making a grant directly than a grant made to the State in which the low-income members reside.

''(C) PRESUMPTION.—If the tribal organization requesting the grant is a tribally designated housing entity (as defined in section 4 of the Native American Housing Assistance and Self-Determination Act of 1996 (25 U.S.C. 4103)) that has operated without material audit exceptions (or without any material audit exceptions that were not corrected within a 3-year period), the Secretary shall presume that the low-income members of the applicable Indian tribe would be equally or better served by making a grant directly to the tribal organization than by a grant made to the State in which the low-income members reside.'';

(2) in paragraph (2)—

(A) by striking ''The sums'' and inserting ''ADMINISTRATION.—The amounts'';

(B) by striking ''on the basis of his determination'';

(C) by striking ''individuals for whom such a determination has been made'' and inserting ''low-income members of the Indian tribe''; and

(D) by striking ''he'' and inserting ''the Secretary''; and

(3) in paragraph (3), by striking ''In order'' and inserting ''APPLICATION.—In order''.

SEC. 204. APPRAISALS.

(a) IN GENERAL.—Title XXVI of the Energy Policy Act of 1992 (25 U.S.C. 3501 et seq.) is amended by adding at the end the following:

''SEC. 2607. APPRAISALS.

''(a) IN GENERAL.—For any transaction that requires approval of the Secretary and involves mineral or energy resources held in trust by the United States for the benefit of an Indian tribe or by an Indian tribe subject to Federal restrictions against alienation, any appraisal relating to fair market value of those resources required to be prepared under applicable law may be prepared by—

''(1) the Secretary;

''(2) the affected Indian tribe; or

''(3) a certified, third-party appraiser pursuant to a contract with the Indian tribe.

''(b) SECRETARIAL REVIEW AND APPROVAL.—Not later than 45 days after the date on which the Secretary receives an appraisal prepared by or for an Indian tribe under paragraph (2) or (3) of subsection (a), the Secretary shall—

''(1) review the appraisal; and

''(2) approve the appraisal unless the Secretary determines that the appraisal fails to meet the standards set forth in regulations promulgated under subsection (d).

''(c) NOTICE OF DISAPPROVAL.—If the Secretary determines that an appraisal submitted for approval under subsection (b) should be disapproved, the Secretary shall give written notice of the disapproval to the Indian tribe and a description of—

''(1) each reason for the disapproval; and

''(2) how the appraisal should be corrected or otherwise cured to meet the applicable standards set forth in the regulations promulgated under subsection (d).

''(d) REGULATIONS.—The Secretary shall promulgate regulations to carry out this section, including standards the Secretary shall use for approving or disapproving the appraisal described in subsection (a).''.

SEC. 205. LEASES OF RESTRICTED LANDS FOR NAVAJO NATION.

(a) IN GENERAL.—Subsection (e)(1) of the first section of the Act of August 9, 1955 (commonly known as the ''Long-Term Leasing Act'') (25 U.S.C. 415(e)(1)), is amended—

(1) by striking '', except a lease for'' and inserting '', including a lease for'';

(2) by striking subparagraph (A) and inserting the following:

''(A) in the case of a business or agricultural lease, 99 years;'';

(3) in subparagraph (B), by striking the period at the end and inserting ''; and''; and

(4) by adding at the end the following:

''(C) in the case of a lease for the exploration, development, or extraction of any mineral resource (including geothermal resources), 25 years, except that—

''(i) any such lease may include an option to renew for 1 additional term of not to exceed 25 years; and

''(ii) any such lease for the exploration, development, or extraction of an oil or gas resource shall be for a term of not to exceed 10 years, plus such additional period as the Navajo Nation determines to be appropriate in any case in which an oil or gas resource is produced in a paying quantity.''.

(b) GAO REPORT.—Not later than 5 years after the date of enactment of this Act, the Comptroller General of the United States shall prepare and submit to Congress a report describing the progress made in carrying out the amendment made by subsection (a).

SEC. 206. EXTENSION OF TRIBAL LEASE PERIOD FOR THE CROW TRIBE OF MONTANA.

Subsection (a) of the first section of the Act of August 9, 1955 (25 U.S.C. 415(a)), is amended in the second sentence by inserting '', land held in trust for the Crow Tribe of Montana'' after ''Devils Lake Sioux Reservation''.

SEC. 207. TRUST STATUS OF LEASE PAYMENTS.

(a) DEFINITION OF SECRETARY.—In this section, the term ''Secretary'' means the Secretary of the Interior.

(b) TREATMENT OF LEASE PAYMENTS.—

(1) IN GENERAL.—Except as provided in paragraph (2) and at the request of the Indian tribe or individual Indian, any advance

payments, bid deposits, or other earnest money received by the Secretary in connection with the review and Secretarial approval under any other Federal law (including regulations) of a sale, lease, permit, or any other conveyance of any interest in any trust or restricted land of any Indian tribe or individual Indian shall, upon receipt and prior to Secretarial approval of the contract or conveyance instrument, be held in the trust fund system for the benefit of the Indian tribe and individual Indian from whose land the funds were generated.

(2) RESTRICTION.—If the advance payment, bid deposit, or other earnest money received by the Secretary results from competitive bidding, upon selection of the successful bidder, only the funds paid by the successful bidder shall be held in the trust fund system.

(c) USE OF FUNDS.—

(1) IN GENERAL.—On the approval of the Secretary of a contract or other instrument for a sale, lease, permit, or any other conveyance described in subsection (b)(1), the funds held in the trust fund system and described in subsection (b), along with all income generated from the investment of those funds, shall be disbursed to the Indian tribe or individual Indian landowners.

(2) ADMINISTRATION.—If a contract or other instrument for a sale, lease, permit, or any other conveyance described in subsection (b)(1) is not approved by the Secretary, the funds held in the trust fund system and described in subsection (b), along with all income generated from the investment of those funds, shall be paid to the party identified in, and in such amount and on such terms as set out in, the applicable regulations, advertisement, or other notice governing the proposed conveyance of the interest in the land at issue.

(d) APPLICABILITY.—This section shall apply to any advance payment, bid deposit, or other earnest money received by the Secretary in connection with the review and Secretarial approval under any other Federal law (including regulations) of a sale, lease, permit, or any other conveyance of any interest in any trust or restricted land of any Indian tribe or individual Indian on or after the date of enactment of this Act.

SA 2715. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. PROHIBITION ON THE INDEFINITE DETENTION OF CITIZENS AND LAWFUL PERMANENT RESIDENTS.

Section 4001 of title 18, United States Code, is amended—

(1) by striking subsection (a) and inserting the following:

''(a) No citizen or lawful permanent resident shall be imprisoned or otherwise detained by the United States except consistent with the Constitution and pursuant to an Act of Congress that expressly authorizes such imprisonment or detention.'';

(2) by redesignating subsection (b) as subsection (c); and

(3) by inserting after subsection (a) the following:

''(b)(1) A general authorization to use military force, a declaration of war, or any similar authority, on its own, shall not be construed to authorize the imprisonment or detention without charge or trial of a citizen or lawful permanent resident of the United States apprehended in the United States.

''(2) Paragraph (1) applies to an authorization to use military force, a declaration of war, or any similar authority enacted before, on, or after the date of the enactment of the Cybersecurity Information Sharing Act of 2015.

''(3) This section shall not be construed to authorize the imprisonment or detention of a citizen of the United States, a lawful permanent resident of the United States, or any other person who is apprehended in the United States.''.

SA 2716. Mr. BURR (for himself and Mrs. FEINSTEIN) proposed an amendment 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:

Strike all after the enacting clause and insert the following:

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.

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 period 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. 532)).

(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 measures 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)); and

(7) 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; and

''(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)).

''(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.—Notwithstanding section 202, in this subsection, 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 all taken 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, 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, as defined in section 11103 of title 40, United States Code; and

(2) the Director of National Intelligence 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.

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 owned 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 use of protective capabilities under the control of the Secretary for communications or other system traffic transiting to or from or stored on an agency information system for the purpose of ensuring the security of the information or information system or other 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''.

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 Armed Services in the House of Representatives;

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

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

(G) 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 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 non-civilian 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 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 203 and 204; 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 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 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 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 2(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 private sector in near real time, at no cost 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.

(e) CYBERSECURITY FRAMEWORK.—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—

(1) establishes a common set of security practices and standards that specifically pertain to a range of health care organizations;

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

(3) is consistently updated and applicable to the range of health care organizations described in paragraph (1).

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 each submit to each Comptroller General of the United States and 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.

(c) GAO ECONOMIC ANALYSIS AND REPORT ON FEDERAL COMPUTER SYSTEMS.—

(1) REPORT.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall submit to Congress a report examining, including an economic analysis of, any impediments to agency use of effective security software and security devices.

(2) CLASSIFIED INFORMATION.—A report 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 under subsection (b).

(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; and

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

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

(b) IDENTIFICATION OF CRITICAL INFRASTRUCTURE AT GREATEST RISK REQUIRED.—No later than 60 days after the date of the enactment of this Act, the Secretary shall identify critical infrastructure entities where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

(c) 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.

(d) 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 intrusion 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.

(e) SENATE OF CONGRESS.—To the extent that the Secretary proposes to require the reporting of significant cyber intrusions of any covered entity pursuant to a recommendation identified in subsection (d) it is the Sense of Congress that—

(1) the Secretary should ensure that the policies and procedures established for such reporting incorporate, to the greatest extent practicable, processes, roles, and responsibilities of appropriate agencies and entities, including sector specific information sharing and analysis centers, that were in effect on the day before the date of the enactment of this Act;

(2) no cause of action should lie or be maintained in any court against a covered entity, and such action should be promptly dismissed for sharing information with the Secretary or the appropriate agency head for sharing such information;

(3) the Secretary or appropriate agency head, as the case may be, should, under section 103 and to the greatest extent practicable, make available to any covered entity submitting a report such cyber threat indicators as the Secretary or appropriate agency head considers appropriate; and

(4) the Secretary or the appropriate agency head (as the case may be) should take such actions as the Secretary or the appropriate agency head (as the case may be) considers appropriate to protect from disclosure the identity of the covered entity.

SA 2717. Mr. UDALL (for himself, Mrs. SHAHEEN, Mr. TESTER, and Mr. MERKLEY) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

SEC. 11. EXTENSION OF LAND AND WATER CONSERVATION FUND.

Section 200302 of title 54, United States Code, is amended—

(1) in subsection (b), in the matter preceding paragraph (1), by striking ''September 30, 2015'' and inserting ''December 11, 2015''; and

(2) in subsection (c)(1), by striking ''September 30, 2015'' and inserting ''December 11, 2015''.

SA 2718. Mr. UDALL (for himself, Mrs. SHAHEEN, Mr. TESTER, and Mr. MERKLEY) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ____. PERMANENT REAUTHORIZATION OF LAND AND WATER CONSERVATION FUND.

(a) IN GENERAL.—Section 200302 of title 54, United States Code, is amended—

(1) in subsection (b), in the matter preceding paragraph (1), by striking ''During the period ending September 30, 2015, there'' and inserting ''There''; and

(2) in subsection (c)(1), by striking ''through September 30, 2015''.

(b) PUBLIC ACCESS.—Section 200306 of title 54, United States Code, is amended by adding at the end the following:

''(c) PUBLIC ACCESS.—Not less than 1.5 percent of amounts made available for expenditure in any fiscal year under section 200303, or $10,000,000, whichever is greater, shall be used for projects that secure recreational public access to existing Federal public land for hunting, fishing, and other recreational purposes.''.

SA 2719. Mr. ALEXANDER submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ____. 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 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 2(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 private sector in near real time, at no cost 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.

(e) CYBERSECURITY FRAMEWORK.—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—

(1) establishes a common set of security practices and standards that specifically pertain to a range of health care organizations;

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

(3) is consistently updated and applicable to the range of health care organizations described in paragraph (1).

AUTHORITY FOR COMMITTEES TO MEET

COMMITTEE ON ENERGY AND NATURAL RESOURCES

Mr. TOOMEY. 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 20, 2015, at 10 a.m., room SD–366 of the Dirksen Senate Office Building.

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

COMMITTEE ON FOREIGN RELATIONS

Mr. TOOMEY. Mr. President, I ask unanimous consent that the Committee on Foreign Relations be authorized to meet during the session of the Senate on October 20, 2015, at 10 a.m., to conduct a hearing entitled ''The Persistent North Korea Denuclearization and Human Rights Challenge.''

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

SELECT COMMITTEE ON INTELLIGENCE

Mr. TOOMEY. Mr. President, I ask unanimous consent that the Select Committee on Intelligence be authorized to meet during the session of the Senate on October 20, 2015, at 2:30 p.m.

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

SUBCOMMITTEE ON MULTILATERAL INTERNATIONAL DEVELOPMENT, MULTILATERAL INSTITUTIONS, AND INTERNATIONAL ECONOMIC, ENERGY, AND ENVIRONMENTAL POLICY

Mr. TOOMEY. Mr. President, I ask unanimous consent that the Committee on Foreign Relations Subcommittee on Multilateral International Development, Multilateral Institutions, and International Economic, Energy, and Environmental Policy be authorized to meet during the session of the Senate on October 20, 2015, at 2:45 p.m., to conduct a hearing entitled ''2015 Paris International Climate Negotiations: Examining the Economic and Environmental Impacts.''

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

THE CALENDAR

Mr. MCCONNELL. Mr. President, I ask unanimous consent that the Senate proceed to the immediate consideration of Calendar Nos. 256, 257, 258, 259, 260, 261, and 262, en bloc.

There being no objection, the Senate proceeded to consider the bills en bloc.

Mr. MCCONNELL. Mr. President, I ask unanimous consent that the bills be read a third time and passed, that the motions to reconsider be considered made and laid upon the table, and that any statements related to the bills be printed in the RECORD, all en bloc.

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

SGT. ZACHARY M. FISHER POST OFFICE

The bill (H.R. 322) to designate the facility of the United States Postal Service located at 16105 Swingley Ridge Road in Chesterfield, Missouri, as the ''Sgt. Zachary M. Fisher Post Office,'' was ordered to a third reading, was read the third time, and passed.

SGT. AMANDA N. PINSON POST OFFICE

The bill (H.R. 323) to designate the facility of the United States Postal Service located at 55 Grasso Plaza in St. Louis, Missouri, as the ''Sgt. Amanda N. Pinson Post Office,'' was ordered to a third reading, was read the third time, and passed.

LT. DANIEL P. RIORDAN POST OFFICE

The bill (H.R. 324) to designate the facility of the United States Postal Service located at 11662 Gravois Road in St. Louis, Missouri, as the ''Lt. Daniel P. Riordan Post Office,'' was ordered to a third reading, was read the third time, and passed.

RICHARD ''DICK'' CHENAULT POST OFFICE BUILDING

The bill (H.R. 558) 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,'' was ordered to a third reading, was read the third time, and passed.

STAFF SERGEANT ROBERT H. DIETZ POST OFFICE BUILDING

The bill (H.R. 1442) to designate the facility of the United States Postal Service located at 90 Cornell Street in Kingston, New York, as the ''Staff Sergeant Robert H. Dietz Post Office Building,'' was ordered to a third reading, was read the third time, and passed.

OFFICER DARYL R. PIERSON MEMORIAL POST OFFICE BUILDING

The bill (H.R. 1884) to designate the facility of the United States Postal Service located at 206 West Commercial Street in East Rochester, New York, as the ''Officer Daryl R. Pierson Memorial Post Office Building,'' was ordered to a third reading, was read the third time, and passed.

JAMES ROBERT KALSU POST OFFICE BUILDING

The bill (H.R. 3059) to designate the facility of the United States Postal Service located at 4500 SE 28th Street, Del City, Oklahoma, as the James Robert Kalsu Post Office Building, was ordered to a third reading, was read the third time, and passed.

NATIONAL CASE MANAGEMENT WEEK

Mr. MCCONNELL. Mr. President, I ask unanimous consent that the Judiciary Committee be discharged from further consideration of and the Senate now proceed to the consideration of S. Res. 261.

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

The clerk will report the resolution by title.

The bill clerk read as follows:

A resolution (S. Res. 261) designating the week of October 11 through October 17, 2015, as ''National Case Management Week'' to recognize the role of case management in improving health care outcomes for patients.

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

Mr. MCCONNELL. I ask unanimous consent that the resolution be agreed to, the preamble be agreed to, and the motions to reconsider be laid upon the table.

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

The resolution (S. Res. 261) was agreed to.

The preamble was agreed to.

(The resolution, with its preamble, is printed in the RECORD of September 22, 2015, under ''Submitted Resolutions.'')

ORDERS FOR WEDNESDAY, OCTOBER 21, 2015

Mr. MCCONNELL. Mr. President, I ask unanimous consent that when the Senate completes its business today, it adjourn until 9:30 a.m., Wednesday, October 21; 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 for 1 hour, with Senators permitted to speak therein; further, that the time during morning business be equally divided, with the majority controlling the first half and the Democrats controlling the final half; finally, that following morning business, the Senate then resume consideration of S. 754.

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

ADJOURNMENT UNTIL 9:30 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 6:19 p.m., adjourned until Wednesday, October 21, 2015, at 9:30 a.m.

CONFIRMATION

Executive nomination confirmed by the Senate October 20, 2015:

THE JUDICIARY

ANN DONNELLY, OF NEW YORK, TO BE UNITED STATES DISTRICT JUDGE FOR THE EASTERN DISTRICT OF NEW YORK.