United States of America

Congressional Record

PROCEEDINGS AND DEBATES OF THE 114th CONGRESS, FIRST SESSION

Vol. 161 WASHINGTON, SUNDAY, MAY 31, 2015 No. 85

House of Representatives

The House was not in session today. Its next meeting will be held on Monday, June 1, 2015, at 2 p.m.

Senate

SUNDAY, MAY 31, 2015

The Senate met at 4 p.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.

O God, our rock and our fortress, thank You for guiding our lives. Without the unfolding of Your loving providence, we would miss life's music. Lord, You have set our feet on solid ground and delivered us from our enemies. You have kept us from sorrow and sighing for we trust You in life's storms.

Today, empower our lawmakers to be instruments of Your will. Remind them that their times are in Your hands as You save them in Your steadfast love. Give them serenity to accept what they cannot change and courage to change what they can.

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 PRESIDENT pro tempore. The majority leader is recognized.

REMEMBERING BEAU BIDEN

Mr. MCCONNELL. Mr. President, I will have more to say about the Senate business before the Senate later, but at this time I wish to express my sincere condolences to the entire Biden family in their moment of such deep and profound loss.

Beau Biden was known to many as a dedicated public servant, a loving father of two, and a devoted partner to the woman he loved, Hallie.

I have known the Vice President for many years, and it is hard to think of anything more important to him than his faith and his family. I hope he will find comfort in the former as he grieves such a terrible loss.

The Senate offers its Presiding Officer and every member of his family our prayers and our sympathy.

ORDER OF PROCEDURE

Mr. MCCONNELL. Mr. President, I ask unanimous consent that the time until 5 p.m. be equally divided in the usual form and that the Senate recess at 5 p.m. subject to the call of the Chair.

The PRESIDENT pro tempore. Without objection, it is so ordered.

RECOGNITION OF THE MINORITY LEADER

The PRESIDENT pro tempore. The minority leader is recognized.

REMEMBERING BEAU BIDEN

Mr. REID. Mr. President, I join in my feelings about the JOE BIDEN family. I was saddened beyond words to hear of the passing of Beau. He was such a fine young man. He was a devoted husband, father, son, a dedicated servant to the people of Delaware, and a faithful, honorable veteran of the United States, having served in the Middle East in Iraq.

I, of course, extend all of the sympathy I am capable of extending to his family during this very difficult time. Beau left us far too soon. He was only 46 years old, but I am certain his family will take solace in knowing he lived a selfless, noble life.

To my friend JOE BIDEN, whom I served with in Congress for so many years, I extend my deepest thoughts and condolences to you, JOE.

There is a song ''Man of Constant Sorrow'' that certainly, if that ever applied to someone, it would be our friend JOE BIDEN. Not having been sworn in to the Senate, he experienced the tragic loss of his wife and little girl. Then, as to his two sons, Beau and Hunter, he spent time on a train going back and forth to Delaware virtually every night so he could take care of those two fine young men until he was fortunate enough to meet Jill Biden, his beautiful wife.

I am very sorry JOE has had to go through this terrible ordeal now of losing a son after having lost a daughter.

But, I repeat, there is no question that Delaware is a better place because of Beau, our country is a better place because of Beau, and the world is better place because of Beau Biden.

I, and the entire Senate family, as Senator MCCONNELL has indicated,

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

Printed on recycled paper.

send our deepest condolences as they grieve during this tragic time.

NATIONAL SECURITY LEGISLATION

Mr. REID. Mr. President, we are here facing yet another manufactured crisis with the vitally important PATRIOT Act provision set to expire in a matter of hours. In fact, we have less than 8 hours before the expiration of this critical national security program. That is what we are faced with.

Tonight's deadline is certainly no surprise. As the junior Senator from Utah, a Republican, noted: ''We've known for four years that this deadline was approaching.''

Like so many other occasions in which brinksmanship has pushed the Senate and our Nation to the precipice, the dilemma we now face was completely avoidable. The job of the leader is to have a plan. In this case, it is clear the majority leader simply didn't have a plan. The majority leader had 5 months to introduce a bill from committee that would reform and extend the expiring PATRIOT Act provisions, but instead he bypassed the committees altogether and brought this to the floor unilaterally, with no committee hearing—none.

The majority leader recently said no more rule XIVs, but that pledge has not lasted very long, has it. The majority leader had, I repeat, 5 months.

In fact, my friend, the ranking member of the Judiciary Committee and a dean of the Senate, said this could have passed so easily in the last 2 years. The majority leader had 5 months during the time he has been the majority leader to coordinate with the House, which passed FISA reform weeks ago, but instead he went it alone.

In fact, it is as if the House and Senate Republican leaders appear to be on different pages. Everyone saw this coming. Weeks ago, it was clear the Senate didn't have adequate time to consider trade legislation, surveillance legislation, and, of course, the highway bill before the Memorial Day recess. I said that and others said that.

Listen to what one Republican Congressman said. His name is REID RIBBLE.

> He could have handled it better by being more prepared in advance for it. They ran out the clock basically by working on trade first; he probably should have ran the clock out on [surveillance] instead. I don't know what his strategy is here. I'm a little bit flummoxed.

I say to my friend, Congressman RIBBLE, that he is not the only one who is flummoxed; so are we.

The Senate majority leader set up a collision course with no plan on how to resolve it. It seems the only plan the majority leader had on FISA was to jam it through last Friday night; this, despite the fact that an overwhelming majority of House Members oppose an extension, the President opposes an extension, and a dozen Senate Republicans oppose an extension and so voted last Friday.

Is it any wonder, then, that even the majority leader's own Republican Senators felt it necessary to take matters into their own hands?

The majority leader was also caught off guard by a Member of his own Republican conference last week who refused to allow the Senate to extend the provisions for a program that the Second Circuit has determined is illegal.

But, again, the junior Senator from Kentucky did not hide his thoughts. He was on the floor for 10 hours or so. I disagree with the junior Senator from Kentucky, but we are not in the mess today because of the junior Senator of Kentucky; we are in the mess we are today because of the majority leader.

The majority leader should have seen this coming. Everyone else did, even those in his own party. Meanwhile, the Republican leader has repeatedly lectured this body as to how it should function, but his actions have helped the Senate to not function.

We can do without more lectures and defiant statements. We can do with more strategy, planning, and open lines of communication because it is the majority leader's job to have a plan and to prioritize what must get done over what he would like to get done.

In this case, my friend from Kentucky simply did not have a plan, and that is why we are here staring down the barrel of yet another unnecessary manufactured crisis that threatens our national security.

We heard what the head of the CIA said today on a Sunday show. He said he is afraid something will happen when this act expires. That is not just my assessment of the situation. This is from the head of the CIA. Senate Republicans even feel the same way.

The Republican junior Senator from Montana said yesterday:

> We could have done this a week ago. And this is the nature of Washington, D.C., always managing by crisis.

Fortunately, there is a clear way out: pass the USA FREEDOM Act, which the House overwhelmingly passed with 338 votes on a totally bipartisan basis. All we need are a few more Republican Senators to vote with Democrats and the bill will pass. Just three, maybe four, maybe five—but a few Senators is all we need to bring this unnecessary crisis to a screaming halt.

I am confident we can pass this bill if the majority leader will bring it to the floor for a fair vote.

Now, procedurally, it is going to be extremely difficult to not have this bill—this law expire. This is not a bill; this is a law that is expiring. Any other course than just passing this bill would require the House to act before midnight. They are not here, so it is not going to happen. There is not a quorum of House Members, and there are House Members who will object to a unanimous consent request anyway.

Passing the USA FREEDOM Act is the only way I can foresee where the PATRIOT Act provisions do not expire. Now is the time for the majority leader to do what is right for the privacy and security of all Americans.

I yield the floor.

RESERVATION OF LEADER TIME

The PRESIDENT pro tempore. Under the previous order, the leadership time is reserved.

USA FREEDOM ACT OF 2015—MOTION TO PROCEED

The PRESIDENT pro tempore. Under the previous order, the Senate will resume consideration of the motion to proceed to H.R. 2048, which the clerk will report.

The senior assistant legislative clerk read as follows:

> Motion to proceed to Calendar No. 87, H.R. 2048, a bill to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes.

The PRESIDENT pro tempore. The minority leader.

Mr. LEAHY. I ask, through the Chair, if the Democratic leader will yield to me for a comment.

Mr. REID. Mr. President, I am happy to yield to the Senator for a comment.

Mr. LEAHY. Mr. President, I was struck by what the Democratic leader said. He laid out the history of this. We are here in a manufactured, unnecessary crisis. It is a manufactured, unnecessary crisis.

Last year, by an overwhelming majority, the Senate voted to make improvements to the PATRIOT Act. The legislation made reforms to the provisions that have now been declared illegal. We did that but could not get past a filibuster. We had 58 votes. Normally, you think of 51 votes being enough to pass a bill. The Democratic leader will recall how hard he worked to try to get that bill through. The Republican leader said: No, we will wait until next year. Well, next year came. We have wasted so much time. There has not been a single public hearing. There has not been any action on an alternative to the USA FREEDOM Act.

But, I say to my friend from Nevada, he is absolutely right when he says the House passed the USA FREEDOM Act by a 4 to 1 margin. It was an overwhelming vote, Republicans and Democrats together, to get rid of the illegal parts of the PATRIOT Act, to pass an improvement. We ought to just take up the USA FREEDOM Act and pass it.

If we were allowed to have a straight up-or-down vote in this body, I guarantee you, a majority of Senators—both parties—would vote for it.

So I just wanted to say that while the leader was on the floor.

I now ask for recognition in my own right.

The PRESIDENT pro tempore. The Senator from Vermont.

Mr. LEAHY. Mr. President, before I begin my comments on the USA FREEDOM Act, I am going to speak for a moment on a personal matter.

REMEMBERING BEAU BIDEN

Mr. President, Marcelle and I have known Beau Biden since he was a child. I am the longest serving Member of this Senate. When I came here, there was one Senator who was one term senior to me; that was JOE BIDEN. I knew of the tragedy his family had gone through, and I cherished the times, with his office right near mine, when his sons Beau and Hunter would be there with him. I watched them grow up. I saw Beau Biden become the epitome of what a State's attorney general should be. That is a model all attorneys general throughout the country could have followed. Progressive, worried about improving the law, improving peoples' lives—he did that.

I know how much we appreciated it when we would see him and Hallie at an event, when Marcelle and I would get a chance to talk with them. It was like picking up a conversation that had ended just a few minutes before.

I remember one thing especially about Beau. I was in Iraq during the war. It was a day when it was well over 100 degrees outside. I was being brought to a place where there was going to be a briefing, being zipped into this building. There were a number of soldiers wearing T-shirts, shorts, and sidearms playing ball outside in this 110-, 120-degree heat. As I went to the door, one of them turned around and gave me a big wave with his arm blocking his face. I was not sure who it was. I kind of waved back. Pretty soon, he came to the door. It was Beau Biden. I remember we gave each other a big hug. He was there as a captain in the Delaware Reserves. He was decorated for his service. We talked about what he was doing. He was praising the men and women who worked there. Nothing about anything he might be doing; he was praising everybody else. It was such a refreshing moment being with him, and it was so typical of who he was as a person.

I told him that I have a procedure that if I am in another country and I am with our military, that if there are Vermonters there, I always take their names and I ask them if they have family back home in Vermont. Most of them do. I get their phone number, and as soon as I get back, I call their mother or their father, their husband or their wife, brother or sister, whoever it might be, and say: I saw a member of your family; here is what they are doing; they look well, and all that.

So I told Beau, I said: Look, I have known you since you were a youngster. I will call your father as soon as I can and tell him you are behaving yourself, and you are doing a good job. We laughed at that.

Shortly thereafter, I got on the phone we had available to us to go through the Whitehouse switchboard to reach the Vice President. Then I started to talk about the procedure I have, and JOE BIDEN started to laugh. He said: I just got an email from Beau that he had seen you there and that I should be expecting a call from you. We talked about what a great job Beau was doing. You could hear the pride in his father's voice. You could hear his pride. It was a pride that was deserved.

I remember JOE saying, when we were first here in the Senate—the two of us—he would be going home every night on the train. Why? Not as much even that the kids needed him, but he needed them.

Finally, when he met Jill, the boys were telling him: You should marry her.

So I grieve for them. Marcelle and I sat there and cried last night when we heard the news. I think, what a wonderful family. I think about a life cut too short—far too short.

Mr. President, I can and will say more later.

Mr. President, on the matter the distinguished Democratic leader was talking about, the USA FREEDOM Act, let's just take it up and pass it. Opponents of this bipartisan, commonsense legislation have run out of excuses. I see this as a manufactured crisis, and it is. This matter should have been taken up and voted on up or down a month ago. There is only one viable and responsible path remaining: Pass the USA FREEDOM Act that passed overwhelmingly in the House of Representatives. Pass it and send it to the President's desk and he will sign it. If we do not pass it, then those parts of the PATRIOT Act that most of us agree on are going to expire at midnight.

The irony of it is that the USA FREEDOM Act of 2015 is a carefully crafted, bipartisan compromise that both protects Americans' privacy and keeps this country safe. Before they were talking about, we are going to keep the country safe but Americans' privacy—not so much. This is a bill that does both.

The legislation would end the NSA's bulk collection of Americans' phone records. It adds significant new reforms to limit government surveillance. It increases transparency and also promotes greater accountability and oversight—something the original PATRIOT Act did not have.

The bill is the product of countless hours of painstaking negotiations with key Members—both Republicans and Democrats—in the House and the Senate, men and women I respect so much because they want to do what is best for the country. We have negotiated with the NSA, the FBI, the Justice Department, privacy and civil liberties groups, the technology industry, and other key stakeholders. We brought everybody together. When we began, we wondered if that would be possible. We did it. That is why the USA FREEDOM Act has such strong support, including from groups as diverse as the National Rifle Association and the Center for American Progress.

This broad consensus is what we saw by the overwhelming support it received in the House. They passed the USA FREEDOM Act by a vote of 338 to 88. Some in this country say that no branch of government could have a vote that strong to say the Sun rises in the east. Certainly there has been no major piece of legislation in years where we have seen a vote such as that—338 to 88.

But now a minority in the Senate has now twice blocked the USA FREEDOM Act from even getting a debate on the Senate floor. We were sent here not to vote maybe but to vote yes or no.

Last November, even though we had had all kinds of committee hearings on this, we heard complaints that there had not been enough of a committee process on the bill and that the Senate should wait to address Section 215 under the new Republican leadership. So the Republican leader led a successful filibuster against a bill which still had a majority of Members in this body voting for it. But what has happened in this Congress? Not a single public hearing on this issue; no committee process. And then last weekend, the Senate was blocked from even debating the House-passed bill and considering amendments.

Opponents of reform have failed to introduce any legislative alternative to the bipartisan USA FREEDOM Act, the bill which reforms many problems of the PATRIOT Act. They have come up with no legislative alternative other than a clean extension, which we know has no chance of becoming law. Of course, it makes no difference because at midnight it stops being the law.

The time for excuses and inaction has passed. The American people and the intelligence community professionals who strive to protect them deserve better.

We have a few hours remaining to work things out and pass the USA FREEDOM Act, but there is no room for error. There is very little time. Again, I said it is a manufactured crisis. The deadline to act is midnight tonight. The House will not return to the Capitol until tomorrow, after the deadline has passed. We could talk about passing a 100-year extension if we wanted; it makes no difference because the time will have passed. So if the Senate does not pass the House-passed USA FREEDOM Act or if we amend it in any way, the authorities are going to expire.

I have said repeatedly—and my cosponsor of the USA FREEDOM Act, Senator LEE, agrees with me—that we would like to have a debate on our bill and consider amendments. Because opponents of reform have run out the clock and jammed the Senate, we are not left with very much time.

Let's get this done today. If we pass the USA FREEDOM Act, the President could sign it tonight and the intelligence community could move forward

with the certainty it needs to protect the American people.

Some may argue that if you had a short-term extension—which, of course, we do not have—they have said: Well, maybe we could work out some kind of a compromise bill. But let there be no misunderstanding: The USA FREEDOM Act is a solid, carefully negotiated compromise. For all those Senators on either side of the aisle who have not spent the hours and hours and hours, as Senator LEE and I and our staffs have spent, maybe they do not know the work that went into this—again, how you get groups from the left to the right supporting it.

It would be irresponsible to kick the can down the road once again, relying on the false hope that the House will agree to pass a short-term extension—something they said they will not do—and that we will somehow be able to agree on a half-baked alternative that has yet to be introduced in either body and most assuredly would not pass the House.

So do not be fooled or tempted by the promise of a short-term extension. That would guarantee nothing. Well, wait a minute. I take that back. Passing a short-term extension does guarantee something: It guarantees the expiration of these authorities at midnight tonight. It guarantees more uncertainty, more litigation, more risk for the intelligence community, and a repeat of the chaotic brinksmanship later on down the road with another manufactured crisis.

I know there are some who worry that the bill does not go far enough when it comes to reform. Well, then where were they in coming up with a better idea? If this passes, the USA FREEDOM Act would be the most significant set of reforms to government surveillance since the PATRIOT Act was enacted. The reason we are here to even debate it is that then-majority leader Dick Armey in the House and I put in sunset provisions. So we will have to show responsibility and vote, as the House did by a 4-to-1 margin.

Our bill—Senator LEE's and my bill—would not just end the NSA's bulk collection under Section 215, it would add new transparency and oversight reforms to other surveillance authorities, and it would be a solid foundation upon which we could build our future reform efforts.

I have been in the Senate for more than 40 years. I have learned that when there is a chance to make real progress, we ought to seize it. But I also know we cannot let this be the end of our fight for greater privacy protections, transparency, and accountability. I remain committed to fighting that fight on behalf of Vermonters and all Americans.

So the choices before us this evening are clear: Either let these authorities expire completely or pass the USA FREEDOM Act. There is no more time for political maneuvering or fearmongering or scare tactics. It is time for us to do our jobs—to debate and then to vote. Don't duck the vote. Vote up or down on the bill the House gave us. Stand up and be counted either for or against it. As Senators, let's have the courage to do that.

The USA FREEDOM Act is a reasonable, responsible way forward, and we should pass it tonight. But don't duck behind not doing anything and pretend that is a solution. I don't think there is a single American, Republican or Democrat, who would believe that was a responsible solution.

Mr. President, I yield the floor.

Ms. MIKULSKI. Mr. President, I am back here during an unprecedented Sunday session hoping we can avoid a totally unnecessary disaster tonight; hoping we will do what is right for the country: Pass the USA FREEDOM Act today. Right now.

I will let others speak to the merits of the USA FREEDOM Act. It is our best opportunity to protect the Nation while balancing between privacy and constitutional surveillance.

I do support reforming the Patriot Act, but I do not support unilateral disarmament of our Nation's need to know what bad guys with predatory intent are planning against the United States of America.

But my comments today are not about standing up for the USA FREEDOM Act.

I am here to stand up for the men and women working for the NSA, FBI, and other intelligence agencies essential to protecting our country against terrorist attacks—whether it is a ''lone wolf'' or state sponsored. These dedicated, patriotic intelligence professionals want to operate under rule of law that is constitutional, legal, and authorized.

They are ready to do their jobs, but Congress needs to do our job and pass a bill that is constitutional, legal, and authorized.

Ever since Edward Snowden made his allegations, the men and women of our intelligence agencies have been vilified as if they were the enemy. They thought they were doing their jobs protecting us against the enemy.

Let me tell you—the men and women of the NSA, FBI, and our other intelligence agencies are patriots who have been wrongly vilified by those who don't bother to inform themselves about our national security structures and the vital functions they perform.

Now a special word about the NSA, which is headquartered in my home State of Maryland. The 30,000 men and women in the NSA serve in silence—without public accolades. They protect us from cyber attacks. They protect us against terrorist attacks. They support our warfighters. They are Ph.D.'s and scientists. They are linguists, cyber geeks, and whiz kids—the treasured human capital of this Nation.

Remember that section 215 is such a small aspect of what the NSA, FBI, and other intelligence agencies do as they stand sentry in cyber space stopping attacks. People act like that is all NSA does. They haven't even bothered to educate themselves as to legality and constitutionality.

Congress passed the Patriot Act. President George W. Bush told us it was constitutional. We need good intelligence. In a world of ISIL, Nusra Front, and al Qaeda, the NSA is our front line of defense and the people of NSA make up that front line.

There is no evidence of abuse by NSA employees. The men and women of NSA have adhered to the law. They have submitted to oversight, audits, checks and balances, and reviews from Congress and the courts.

The employees of NSA know that everything has to be constitutional, legal, and authorized. They thought they were implementing the law, but some in the media and even some in this body have made them feel like they were wrongdoers. I find this infuriating and insulting. Morale has been devastated at NSA. Families have been harassed for working at the NSA and their kids are bullied at school.

They have also been devastated by actions of their own government. First, by sequester—then, by the government shutdown. Now, by Congress's failure to reform national security authorities that help them keep our country safe.

It is wrong. I want people to remember that tonight as we discuss important reforms. Let us not let them down, once again, with our own failure to act.

Mrs. FEINSTEIN. Mr. President, it is greatly disappointing that the Senate is in session today to reconsider a vote we took before the Memorial Day recess to extend the three expiring provisions of the Foreign Intelligence Surveillance Act.

Instead of passing the USA FREEDOM Act a week ago and sending it to the President, we are now poised to take the measure up this coming week, after the FISA authorities have expired. The result is that our intelligence agencies will lose important tools to protect against terrorist attacks. This is a self-inflicted harm, and one that was totally unnecessary.

As I did a week ago, I will vote to invoke cloture on the motion to proceed to the USA FREEDOM Act, and I intend to vote for the legislation through the upcoming procedural votes. The bill is not perfect, but it extends the business records, lone wolf, and roving wiretap provisions and it institutes some important reforms to FISA.

Unfortunately, what we have on the floor of the Senate tonight is political gamesmanship at its worst. We should have had this debate weeks or months ago, not up against the deadline. Failing that, the majority should not have defeated this motion last week when it is prepared today to pass it.

We should skip the unnecessary delay of voting separately on the motion to proceed, cloture on the bill, and on the bill itself. Clearly there are 60 votes in

this chamber to pass the USA FREEDOM Act, whether we do it today or if we do it next week.

So the question comes: why not pass this bill today, reform the business records provision of FISA, and keep important intelligence authorities in effect? Unfortunately, the answer is that one Senator is holding this process hostage for his own political benefit. It is a travesty, and it is unconscionable.

We remain a nation under threat of terrorism. Our allies remain under threat of terrorism.

This is not hypothetical. The Islamic State in Iraq and the Levant—ISIL—is seeking to recruit individuals to conduct attacks against the United States. Tens of thousands of foreign fighters have entered Iraq and Syria to join ISIL. There are hundreds of people inside the United States right now that ISIL is seeking to inspire, direct, and assist in carrying out an attack.

Al Qaeda in the Arabian Peninsula—AQAP—is developing non-metallic, undetectable bombs for use on U.S. airliners and is teaching people how to make such devices themselves. These groups are competing to be worst of the worst in international terrorism and they are coming after us.

We aren't sending thousands of troops to confront ISIL in Iraq and Syria or to stop AQAP in Yemen. We aren't going to diminish their threats through partnership with local governments.

The only way we are going to stop attacks against the United States and our people is by collecting good intelligence. To me, that means we need to do everything lawful and effective in intelligence to identify and thwart those attacks.

The roving wiretap provision is important. It says that the FBI doesn't have to stop surveillance against a terrorist or a foreign spy when he buys a new cell phone or changes his email account. Having to do so in today's world would be ridiculous.

The ''lone wolf'' provision is important. To be clear—it hasn't been used. But to be equally clear, never before have we faced the exact threat that this provision was written to address: the threat of an individual, inside this country, plotting to kill Americans without traveling abroad and training with a terrorist group first.

The business records provision is important. It includes both routine requests for records—hotel bills, car rentals, travel information—that are regular parts of law enforcement and national security investigations. It also authorizes the NSA's phone metadata program. Under this provision, the NSA gets information about phone calls to include the numbers on either end of the line, the time, and the duration of the call. It does not include the words that are spoken as part of the phone conversation, the identities of the people involved, or their location.

What it does is help the Intelligence Community know more about people for whom there is a ''reasonable articulable suspicion'' of being tied to terrorist groups. If there is a terrorist in Syria talking to Americans at home, we want to know that. If a phone number, for example, in Garland, TX, is in touch with an ISIL operations chief, we need to know. That information allows the FBI to go to a court for a probable cause warrant to conduct electronic and physical surveillance of a suspect.

This program is conducted under strict oversight and operational limitations. The number of people at NSA with access to the data is small—it was 22 in 2013. They have to get approval each time they do a query of the phone records; today that approval comes from the FISA Court. The query only returns information on what numbers were called by, and called, the phone number in question, and then a second hop from that number. There were 288 phone numbers approved for queries in 2012, and those queries led to 12 probable cause warrants by the FBI.

The program is overseen within the NSA by multiple officials, including the inspector general and the privacy and civil liberties officer. It is overseen by the Department of Justice, which reviews every single query, and by the Office of the Director of National Intelligence. It is overseen by the Intelligence and Judiciary Committees of the House and the Senate, and it is overseen for compliance purposes by the FISA Court.

So these are important tools that, because of Senate inaction and recalcitrance, will expire tonight. As a result, we make ourselves more vulnerable.

I very much regret this situation that the Senate has created, and I urge my colleagues to vote for cloture and to quickly enact the USA FREEDOM Act.

The PRESIDING OFFICER (Mr. GRASSLEY). The Senator from Indiana is recognized.

Mr. COATS. Mr. President, I also regret that we are where we are.

REMEMBERING BEAU BIDEN

I would also like to defer for just a moment, before I make my remarks that I came to the floor to make, to add my condolences to Vice President BIDEN, his wife, and his family. I just learned the tragic news this morning. Some may have known that Beau was dealing with a form of cancer. I did not know that. It came as a shock to hear that information.

Having served with the current Vice President in the U.S. Senate and having gotten to know him and his family, establishing a relationship—a professional relationship as well as a friendship—I still cannot begin to comprehend the grief that comes from the loss of a child. I know there are Members in this body who have experienced that. I am fortunate that Marsha and I have not experienced that. But any parent's perhaps deepest fear is that they will outlive their children. That is not the natural order of things. It is not how we think. And the grief that comes from the death of a child, the death of a son or a daughter, is truly deep and has significant impact.

It was impossible not to feel the emotion and shed tears early this morning in our home in Indianapolis when we heard the news. Our condolences and deep sharing of grief that we can't even begin to fully comprehend because we haven't had to deal with it—all of that comes across. I think every Member of this body reaches out to them with our thoughts and our prayers as they go through this very tragic situation.

Mr. President, I am a little surprised to hear the Senator from Vermont talking about how the Senate ought to just completely concede to whatever the House sends to the Senate. The fact is that we had a very significant discussion and debate on this issue all week before the Memorial Day break and it had gone on for months, if not years, before in the Intelligence Committee on which I serve and among Members generally.

This is one of the most important pieces of legislation we will have to deal with. It was drafted and spawned as a result of 9/11 when the American people said: Are we doing everything we possibly can to prevent something such as this from happening again?

Congress debated extensively the PATRIOT Act and the tools the intelligence community suggested we give them the authority to use to try to prevent that catastrophe from ever happening again and doing everything we could to prevent terrorist attacks. Along the way, there have been modifications, and there have been changes.

Recently, there has been significant national debate over whether one of these many essential tools that help us gather the intelligence to try to prevent and to understand the nature of the threat should be used. There clearly is a difference of opinion among Members here in the Senate and even in the House of Representatives. Yes, the Senate did pass a reform measure that I think is flawed, personally. I think it diminishes—it doesn't eliminate, but it diminishes and some even believe it eliminates the usefulness of this particular program. We went back and forth on that for a significant part of the week before we adjourned.

The Senator from Vermont comes to the floor and basically says: Look, the House passed this; so therefore we ought to just go ahead and pass it. He said there was no other alternative presented, but that is not the case. We had a procedural vote on the House bill, and we had a vote on the bill to extend this program, so we can come spend a little more time to try to figure out how best to deal with this issue. Neither of those passed, indicating that the Senate did not have the same consensus the House reached, which was a partial consensus. That is what the Senate is all about. We are not just a rubberstamp for the House.

What is really ironic is the fact that for 4 years, under Democratic leadership of this Senate, the House, under Republican leadership, sent us hundreds of pieces of legislation, and if we followed the admonition to us of the Senator from Vermont, we would have just rubberstamped those. The House passed it, so why wouldn't we go forward? I don't think that argument makes a lot of sense.

Senators are here to address issues in the U.S. Senate. Are there many bills the House passes that I agree with? Yes. My party controls the House. Are there bills here that I don't agree with that they have passed? Yes. We, as Senators, use our prerogative in terms of where we stand, and ultimately we take a vote and we either win or we lose. Sometimes it coordinates with the House of Representatives and other times it doesn't, so then we go to conference and we pass an alternative. But to say there hasn't been debate relative to this program in the House-passed bill is simply not true.

Unfortunately, there has been such a significant misrepresentation of what this program is and what this program isn't, and that has caused a lot of angst which we are trying to deal with. Much of the public—at least some portion of the public—is convinced that the government is listening to every phone call they make. It has been said on this floor that they are listening to all our phone calls, that they are collecting all kinds of data. They know everything about us. That is the furthest from the point of this program and the operation of this program that we can conceive of. Yet, a portion of the public has been led to believe that Big Government is in their bedroom, in their house, in their car, in their phone, and tracks them wherever they go; that they are collecting everything about people, including what they buy at Costco and the movies people rent through Netflix. Private industry does collect that kind of stuff, but it is not the government. It is not done under this program.

As a member of the Intelligence Committee, I can tell my colleagues that we have spent hundreds of hours dealing with this program to ensure that it doesn't violate anyone's privacy. It has more oversight through all three branches of government. The executive branch, the judicial branch, and the legislative branch oversee this program. There are six layers within NSA itself that it has to go through, that attorneys have to look at, that legal experts have to look at before they can even proceed to suspect and then take that suspicion to a court to have a judge say: Yes, you might have something here.

It has been said and it is true that unless a person's phone number is in communication with a foreign phone number that is at least strongly suspected of belonging to a terrorist organization—and ultimately the court has to make that decision—a member of Al Qaeda, ISIS, or some group overseas that is attempting to do harm to the United States—why is this particular phone number—not the name of the person who owns the phone number—why is this particular phone number being called by someone in Yemen or being called by what we strongly suspect is a foreign operative through ISIS, Al Qaeda, Yemen, or other points where we know terrorist activity is rampant?

There is a signal that comes up that matches phone numbers, and they say: We better look into this. But before they can look into it, it has to be vetted by a court. It has to be taken to a FISA Court or an intelligence court and judged by that court as something viable to pursue. At that point, it is similar to what a court would order if there were a warrant to go and find more information to see whether this suspicion actually is reality.

We read about it every day and we watch it on television—''Law and Order'' and all the shows and so forth—about how law enforcement suspects that this particular activity is a criminal organization or this is a drug house or they have reason to believe the perpetrator of the crime is this individual. They can't go raiding their house. They can't go downloading information about them until they go to a court and receive approval from a judge saying: Yes, here you are, here is your warrant. You can go and check this out.

Well, this intelligence program is based on the same principle; that is, nobody can collect any information on anybody unless that court approves that operation. Then it is turned over to the FBI, and they look to see if it is the real thing. It is a tool that has been of importance and has been a contribution to our ability to address the potential of terrorist threats and to thwart them before they happen. It has always been used as a way of proving the negative; that is, no, this is OK, we don't need to follow up on this.

The best example is the Boston bombing. When the Tsarnaev brothers' phone was accessed and it was run against the numbers, there was some suspicion that additional terrorist activity would take place in New York. It was proven that was not the case because there were no connections made. So it became a valuable tool in that regard. Instead of shutting down New York, putting them on a high terrorist alert—perhaps the Nation's largest economy in operation there—we were able to quickly determine that wasn't the case.

In response to those who basically say this has never stopped a terrorist attack, two things: No. 1, this is one of the many methods we use to collect the threads of intelligence that come from different sources to try to put together a mosaic or a puzzle as to whether this is something we need to deal with and take seriously. It is a major piece of that puzzle we obtain from the 215 program, which is the collection of phone numbers. We do not collect the names of people who own those numbers. It is the collection of what is called metadata. It has been described as simply the same data that is on our telephone bills that the Supreme Court has said is not a breach of the Fourth Amendment. It is not privileged for privacy purposes. It shows the date the call was made, the duration of the call, the number that was called, and that is it. And those numbers are put into a system whereby we can check against that a number that suspiciously is talking to a foreign operative in a foreign country. That then automatically triggers that you better look at this—it is kind of a ping—you better look at this one. Nobody has access, at this point, to any content related to the name of the individual until it reaches a level of suspicion that is vetted through six layers of oversight and then is sent to a court that looks at it to say: We agree with you or we don't agree with you. And if we agree with you, then it is the FBI who is alerted that they better look into this.

Now, there has never been a time since 9/11 when we have dealt with a higher threshold than we currently are dealing with. You hear about it every day. You read about it every day. ISIS has recruited more than 20,000, it is estimated—significantly more than that are those from 90 different foreign countries. It has made a direct threat toward the United States and its citizens. It is sponsoring and encouraging individuals to not only come over and train and join ISIS and then come back here and wreak havoc on the American people; it is also inspiring those, saying if you don't want to travel over here, just go out and kill somebody. Join the jihad from afar. You can be a part of what we are trying to accomplish simply by doing your own thing. We saw that happen down in Texas. We will see that in other places as people are inspired through ISIS, for whatever sick reason, to take up arms, to cause destruction, and to randomly kill and wreak havoc on the American public.

It has been offered that the House fix—the reform, which did have bipartisan support and did pass the House without a lot of debate—is the solution to this problem. Some agree it goes too far; some agree it doesn't go far enough. But there are problems with that particular FREEDOM Act, which the Senator from Vermont says is the golden grail here and will solve all the problems.

It is clear, and it is the testimony we have received from numerous officials in the counterterrorism business and in the intelligence business, that there are issues with this so-called FREEDOM Act fix that could render—well, No. 1, that do render the program less effective and could render it totally inoperative.

The fact that the NSA has not yet been able to come up with a program

which would ensure that we could have the kind of collection we need in the timeframe we need it—some of this is urgent, some of this is pending, some of this is imminent, and it already goes through layers that delay coming to a conclusion and this adds more.

Also, they have indicated the system is untested and exists in name only. We don't know how the new program would be implemented and we don't know how it would be operated. That is why many of us said: Look, for whatever reason, yes, we are at this point, and, yes, it expires at midnight. What we were trying to do before we left was get a short-term extension. We were negotiating. We think it should have been for a significant amount of time, until NSA could test out its program, but we were willing to go much less than that so we could have an opportunity to come back and debate this further and get to the bottom of some of the misrepresented information that has been sent out to the American people and have an opportunity to counter that and also work together to find ways, through working with the House of Representatives, to come up with a more effective bill that wouldn't put the country in more jeopardy or, as some experts have said, would undermine the entire program.

We obviously will be less agile with the House bill. It requires an expansive regulatory system to amass the level of oversight over the current program. I think the real problem is it requires no data retention mandate. The USA FREEDOM Act does not require companies to hold the data sought by the government. Therefore, the USA FREEDOM Act could be operationally useless as companies update their business model in response to changes in technology or market demand. The telephone companies—all 1,400 of them—many don't want to go through the expensive process of the oversight they need to have in the process. They want to sell phones. And they are hearing a lot from customers who basically say: I don't want to buy your phone if it is going to be subject to them listening to everything I do and say—being collected.

Well, first of all, that is factually wrong, but it is an error that has been said over and over on this floor by some Members. That is absolutely wrong. It is false. If we are going to go forward here, we need intellectual honesty about what the program is and what it isn't, and it shouldn't be labeled as something it isn't. I will address that at a later point in time.

But the USA FREEDOM Act, by not allowing retention for a fixed period of time, also lessens our ability to make this program effective. So I have much more to say on this, and I know we are going into caucus as a party to see how we might go forward, given where we are.

It was not necessary that we be here on a Sunday with the clock ticking toward midnight. We could have continued or we could have gone forward without getting to this particular point in time. But now we will have the opportunity—and, unfortunately, what it looks like is we will have the opportunity to debate this while the program expires.

That is a bet I didn't want to take—the bet being that nothing will happen if we don't have this tool in the amount of time that is going to be taken to now address this. That is running a risk I am not sure Members want to take. I don't want to be part of somebody who says this isn't important enough; therefore, we will let it expire and we will not extend it for a day or an hour or a month or a sufficient amount of time to come to a reasonable conclusion as to how we retain this very important intelligence-gathering tool to keep us safe from terrorists. To go dark on this is a risk of Americans' lives. It is a risk that we are taking, and we are going to be responsible for our vote, whatever that vote is. I, personally, don't want the responsibility of saying: Oh, don't worry. Nothing is going to happen out there. The hundreds of hours that I spend in the Intelligence Committee tells me there is a lot that can happen out there.

Members have every right, if they are not on that committee—every right to access what we access. We have invited people to come down and see it for themselves, so they at least understand what it is and what it isn't. To my knowledge, only two have taken us up on that. There may be more I have missed. But some of those who have stated this program in a totally false way have the siren song to the people out there who think Big Government is in their bedroom, Big Government is taking every piece of information they have about themselves, and Big Government is storing this and ''listening to all your phone calls.'' That is a bunch of hokum and it is wrong.

And for those who refuse to stand up and acknowledge that—because they have had access to the program and refused to take that access—have to bear the responsibility of sowing this wild theory and idea about Big Government in your bedroom and Big Government in your car and Big Government on your phone and Big Government collecting your emails and Big Government doing everything and storing it until the time that Big Government will come and take everything away from you.

I didn't come here to do that and this Senate isn't here to do that and we will not do that. That is why this program has more oversight than any other program in the entire United States Government, and we will put more oversight on there if that is necessary. I will stay up all night and stand over at NSA and make sure they are not listening to your phone calls. But it is irresponsible misrepresentation—irresponsible misrepresentation—to factually state a falsity and not tell the truth.

It is time we told the truth and it is time we stood up to this thing and make sure we are doing everything we can to protect Americans from threats of a lot of people and a lot of organizations that want to kill us all, that would like to see our heads on the chopping block. This is real in our country, as people who are trained by ISIS not only flock back here from Syria, but they inspire people here to pick up weapons and do harm to the American people.

I know the Senator from Arizona has a question.

Mr. PAUL addressed the Chair.

Mr. COATS. I have not yielded the floor.

Mr. PAUL addressed the Chair.

Mr. MCCAIN. Mr. President, I ask for the regular order, and I want to ask the Senator from Indiana a question.

The PRESIDING OFFICER. The Senator from Indiana has the floor.

Mr. COATS. I would be happy to yield to the Senator from Arizona for a question.

Mr. MCCAIN. Maybe the Senator from Kentucky should know the rules of the Senate, that the Senator from Indiana has the floor and the gentleman is open to respond to a question.

My question to the Senator from Indiana—and I want to say that his words are powerful and accurate.

Mr. PAUL. Mr. President, how much time remains on the clock for the Republican side?

Mr. MCCAIN. I would ask the Senator from Indiana if he has seen—

Mr. PAUL. Mr. President, how much time is remaining?

Mr. MCCAIN. I ask for the regular order.

The PRESIDING OFFICER. I think the Chair has made very clear that the Senator from Indiana has the floor.

Mr. COATS. Mr. President, I thank you.

I know the Senator from Kentucky understands that when a Senator has the floor, they are entitled to speak because he has used that rule himself.

Mr. MCCAIN. Twice the Senator from Kentucky has not observed the rules of the Senate.

I would ask the Senator from Indiana, you have seen the events lately that are transpiring. ISIS has taken Palmyra. They are in the streets burning bodies, killing people, going to destroy 2,000-year-old antiquities, and at the same time Ramadi has fallen with thousands of innocent men, women, and children being massacred. At this time, isn't this program as critical as it has ever been since its inception, given the fact that the Middle East is literally on fire and we are losing everywhere?

Mr. COATS. It is more essential than ever, in response to the question from the Senator from Arizona. It is more necessary than ever, as we have seen a higher threat level since 9/11. Of course, we didn't know what the threat was in 9/11, so I don't know how far we have to

go back. But our intelligence today, whether it is any aspect of any of our intelligence agencies, they are sounding the alarm that we need to be as vigilant as possible. We need to, within the law—and we are operating within the law—use every tool possible to try to stop an attack on the American people. What happened on 9/11 was a catastrophe that none of us could have comprehended. A 9/11 with the possession of nuclear, radioactive, biological or chemical weapons would make New York look like just a small incident. It would be 3 million people instead of 3,000 people. I think we have an obligation to do what we can without invading anyone's privacy.

What we are trying to find is this balance between protecting privacy and protecting ourselves from terrorist attacks—protecting Americans from terrorist attacks. We have done this with this program. If what has been said about this program were true, if the falsehoods that have been said were true, I would be the first to line up and say: No, we can't breach the privacy of the American people by doing what they are doing. But the fact is none of it is true. There has not been one act of abuse of this program over the years it has been in place. It has more oversight and layers of oversight. As former Attorney General Mukasey said: For the government to violate and bypass this, it would make Watergate look like kindergarten activity. It would be a conspiracy that would include hundreds of people, and they would all have to swear that they would not breach their conspiratorial process here—a program that is overseen by the Judiciary Committee, by the Senate Intelligence Committee, the House Intelligence Committee, the body of the Senate has access to this and the body of the House—that is 535 people—by the executive branch, a program that was endorsed by Barack Obama, until he changed his mind, apparently, because the public was going the other way based on false information. People are out here basically making the accusations that they are making to try to take this program down and all we are trying to do is work with the House to find a reasonable way of keeping this tool alive—keeping Americans safe.

Mr. MCCAIN. Will the Senator yield for a further question?

The PRESIDING OFFICER. Would the Senator suspend?

Under the previous order, all time for debate has expired.

Mr. PAUL. Mr. President, my understanding is there is still 5 minutes remaining on the opposition side. I request that time.

The PRESIDING OFFICER. Is there objection?

Mr. MCCAIN. I object.

Mr. PAUL. Mr. President, how can we have an objection when we already have a consent agreement that says we have 30 minutes of equally divided time and you still have 5 minutes remaining on the opposite side?

The PRESIDING OFFICER. The time was divided in the usual form, and the time for debate has expired.

Mr. PAUL. Mr. President, the time could not have been divided equally, because apparently somebody must have given one side more time than the other.

The PRESIDING OFFICER. The 5 minutes of time that was allotted to the Democratic side was unused, and it was equally divided at 23 minutes apiece.

Mr. PAUL. Mr. President, I was here for 30 minutes of the Republican side speaking. I sat at my seat for 30 minutes. It was not 23 minutes of equally divided time.

Mr. MCCAIN. Mr. President, regular order—obviously people don't know the rules of the Senate. Maybe they should learn them.

Mr. PAUL. Mr. President, I request the remaining 5 minutes of time on the opposite side.

The PRESIDING OFFICER. Is there objection to the request of the Senator from Kentucky?

Mr. MCCAIN. I object.

Mr. PAUL. Mr. President, I challenge the ruling of the Chair and request the yeas and nays.

The PRESIDING OFFICER. Is there a sufficient second?

There is not a sufficient second.

Mr. PAUL. I request a live quorum call.

The PRESIDING OFFICER. The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

Mr. PAUL. 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. PAUL. Mr. President, I ask unanimous consent to speak for 5 minutes—the 5 minutes that was remaining on the opposition side.

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

Mr. PAUL. Mr. President, let us be very clear about why we are here this evening. We are here this evening because this is an important debate. This is a debate over the Bill of Rights. This is a debate over the Fourth Amendment. This is a debate over your right to be left alone. Justice Brandeis said that the right to be left alone is the most cherished of rights. The right to be left alone is the most prized to civilized men.

Let us be clear. We are here tonight because the President continues to conduct an illegal program. The President has been rebuked by the court. In explicit terms, the President has been told that the program he is conducting is illegal. Now, the President opines on television. The President wants to blame—he says: Anybody but me.

But you know what. The President started this program without congressional permission. Even the authors of the PATRIOT Act say that the PATRIOT Act in no way gives authority to the President to collect all of your phone records all of the time. If there ever was a general warrant, if there ever was a generalized collection of information from people about whom there is no suspicion, this is it.

We are not collecting the information of spies. We are not collecting the information of terrorists. We are collecting all American citizens' records all of the time. This is what we fought the Revolution over. Are we going to so blithely give up our freedom? Are we going to so blithely go along and just say: Take it. Well, I am not going to take it anymore. I do not think the American people are going to take it anymore.

Eighty percent of those under 40 say we have gone too far—that this whole collection of all of our records all the time is too much. The court has said: How can records be relevant to an investigation that has not started? The court has said that even under these lower standards, even under these standards of saying that it would be relevant, all of the stuff they are collecting is precisely irrelevant.

Now people say: Well, they are not looking at it. They are not listening to it. It is the tip of the iceberg, what we are talking about here. Realize that they were dishonest about the program until we caught them. They kept saying over and over: We are not doing this. We are not collecting your records.

They were. The head of the intelligence agency lied to the American people, and he still works there. We should be upset. We should be marching in the streets and saying: He has to go. We cannot allow this. We cannot allow the rule of law to be so trod upon that we live in an arbitrary governmental world where they collect anything they want anytime they want.

This is the tip of the iceberg. They are collecting records through Executive order. They are collecting records through section 702. People say: How will we protect ourselves without these programs? What about using the Constitution? What about using judicial warrants? About the Tsarnaev boy, the Boston Bomber, they say: How will we look at his phone records? Get a warrant. Put his name on it. You can get a warrant. There is no reason in the world—the guy had already bombed us. Do you think anybody was going to turn down a warrant? We should have gotten a warrant before.

Get warrants on people we have suspicion on. The Simpson guy that was shot in Garland had already been arrested. We had suspicion.

Let's hire 1,000 more FBI agents. Let's hire people to do the investigation and quit wasting time on innocent American people. Let's be very clear why we are here: President Obama set up this program, the President Obama who once was against the PATRIOT Act. President Obama once said: You know what; we should have judges write warrants.

President Obama, who once believed in the Fourth Amendment, is the President who is now scooping up all of your records illegally. Then he feigns concern and says: Oh, we need to pass this new bill. He could stop it now. Why won't someone ask the President: Why do you continue? Why won't you stop this program now? The President has every ability to do it. We have every ability to keep our Nation safe. I intend to protect the Constitution.

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

RECESS

The PRESIDING OFFICER. Under the previous order, the Senate stands in recess subject to the call of the Chair.

Thereupon, the Senate, at 5:11 p.m., recessed subject to the call of the Chair and reassembled at 6:14 p.m. when called to order by the Presiding Officer (Mr. WICKER).

USA FREEDOM ACT OF 2015—MOTION TO PROCEED—Continued

The PRESIDING OFFICER. The majority leader.

Mr. MCCONNELL. Mr. President, before the recess, I tried to get a short-term extension of three provisions that will expire at midnight tonight: section 215, business records; section 206, roving wiretap authority; and the ''lone wolf'' provision. Unfortunately, those efforts were unsuccessful.

''Lone wolf'' and roving wiretap are not—I repeat, not—the subject of controversy with the House bill. So I would propose that we extend at least the ''lone wolf'' and the roving wiretap authorities while we continue to litigate the differing views on section 215. More specifically, I would propose that we extend those two provisions—''lone wolf'' and roving wiretaps—for up to 2 weeks.

UNANIMOUS CONSENT REQUEST

Mr. President, having said that, I ask unanimous consent that the Senate proceed to the immediate consideration of a bill, which is at the desk, to extend the expiring provisions relating to ''lone wolf'' and roving wiretaps for 2 weeks, and that the bill be read a third time and passed, and the motion to reconsider be considered made and laid upon the table with no intervening action or debate.

The PRESIDING OFFICER. Is there objection?

The Senator from Kentucky.

Mr. PAUL. Mr. President, reserving the right to object, one of the promises that was given when the PATRIOT Act was originally passed was that, in exchange for allowing a less than constitutional standard, we would only use the actions against——

The PRESIDING OFFICER. Is there objection?

Mr. PAUL. Terrorists and against foreigners. We found that 99 percent of the time, section 213 is used for domestic crime. I believe that no section of the PATRIOT Act should be passed unless our targets are terrorists—not Americans.

Mr. CORNYN. Mr. President, regular order.

The PRESIDING OFFICER. The Senator from Kentucky——

Mr. COTTON. Regular order.

Mr. PAUL. I object.

The PRESIDING OFFICER. Objection is heard.

Mr. MCCONNELL. Mr. President, last week, I proposed giving the Intelligence Committee the time it would need to work toward the kind of bipartisan legislative compromise Americans deserve—a compromise that would preserve important counterterrorism tools necessary to protect American lives. That effort was blocked.

Just now, I proposed an even narrower extension that would have only extended some of the least controversial—least controversial—but still critical tools to ensure they do not lapse as Senators work toward a more comprehensive legislative outcome. But even that very narrow offer was blocked. I think it should be worrying for our country because the nature of the threat we face is very serious. It is aggressive, it is sophisticated, it is geographically dispersed, and it is not—not—going away.

As the LA Times reported, ''the Obama administration has dramatically stepped up warnings of potential terrorist attacks on American soil after several years of relative calm.'' The paper reported that this is occurring in the wake of ''FBI arrests of at least 30 Americans on terrorism-related charges this year in an array of 'lone wolf' plots.''

So these aren't theoretical threats. They are not theoretical threats. They are with us every day. We have to face up to them. We shouldn't be disarming unilaterally as our enemies grow more sophisticated and aggressive, and we certainly should not be doing so based on a campaign of demagoguery and disinformation launched in the wake of the unlawful actions of Edward Snowden, who was last seen in Russia.

The opponents of this program have not been able to provide any—any—examples of the NSA abusing the authorities provided under section 215. And the record will show that, in fact, there has not been one documented instance of abuse of it.

I think it is also important to remember that the contents of calls are not captured. That is the general view, but it is an incorrect one. I will say it again: The contents of calls are not captured. I say this to the American people: If you have been told that, that is not correct. That is what I mean about a campaign of disinformation. The only things in question are the number dialed, the number from which the call was made, the length of the call, and the date. That is it. That is it. Detailed oversight procedures have been put in place, too, in order to protect the privacy of Americans.

Now, I believe this is a program that strikes a critical balance between privacy on the one hand and national security on the other. That doesn't mean the Senate still shouldn't have the opportunity to make some changes to it. That is precisely the outcome I had been hoping to facilitate by seeking several short-term extensions. And considering all that has come to light about the House-passed bill in recent weeks, I believe this was more than reasonable.

The administration's inability to answer even the most basic questions about the alternate bulk data system it would have to build under that legislation is, to say the least, pretty troubling—pretty troubling. And that is not just my view. That is the view of many in this body, including colleagues who have been favorably predisposed to the House bill.

In particular, I know Senators from both parties have been disturbed by the administration's continuing inability to guarantee whether the new system would work as well as the current one or whether there would even be any data available to analyze. While the administration has let it be known that this nonexistent system could only be built in time if telephone providers cooperated in building it, providers have made it abundantly clear that they are not going to commit to retaining the data. They are not going to commit to retaining the data for any period of time unless legally required to do so, and there is no such requirement in the House-passed bill—none at all.

Here is how one provider put it: ''[We are] not prepared to commit to voluntarily retain documents for any particular period of time pursuant to the proposed USA Freedom Act if not required by law''—if not required by law.

Now, these are just a few of the reasons I thought it prudent to try to give the Senate more space to advance better legislation through committee consideration and regular order, with input from both sides. But, my colleagues, it is now clear that will not be possible in the face of a determined opposition from those who simply wish to end the counterterrorism program altogether. No time to try to improve the House-passed bill will be allowed because some would like to end the program altogether.

So this is where we find ourselves. This is the reality. So it essentially leaves us with two options. Option one is to allow the program to expire altogether without attempting to replace it. That would mean disarming completely and arbitrarily, based on a campaign of disinformation, in the face of growing, aggressive, and sophisticated threats—growing, aggressive, and sophisticated threats. That is a totally unacceptable outcome—a completely and totally unacceptable outcome. So we won't be doing that.

So we are left with option two, the House-passed bill. It is certainly not ideal. But along with votes on some modest amendments that attempt to ensure the program can actually work as promised, it is now the only realistic way forward. So I remain determined to continue working toward the best outcome for the American people possible under the circumstances.

This is where we are, colleagues. We have the House-passed bill with some serious flaws and an inability to get a short-term extension to try to improve the House-passed bill in the way we normally do this—through some kind of consultative process.

So bearing that in mind, I move to proceed to the motion to reconsider vote No. 194, the vote by which cloture was not invoked on the motion to proceed to H.R. 2048.

The PRESIDING OFFICER. The question is on agreeing to the motion.

The motion was agreed to.

Mr. MCCONNELL. Mr. President, I move to reconsider the motion to invoke cloture on the motion to proceed to H.R. 2048.

The PRESIDING OFFICER. The question is on agreeing to the motion.

The motion was agreed to.

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 H.R. 2048, an act to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes.

Mitch McConnell, Lamar Alexander, Michael B. Enzi, David Vitter, John Cornyn, Johnny Isakson, Lisa Murkowski, John Barrasso, Richard Burr, Pat Roberts, Roy Blunt, Bob Corker, Orrin G. Hatch, Jerry Moran, Patrick J. Toomey, Mike Lee, Ted Cruz.

The PRESIDING OFFICER. 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 H.R. 2048, an act to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes, shall be brought to a close, upon reconsideration?

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 Senators are necessarily absent: the Senator from Wyoming (Mr. ENZI), the Senator from South Carolina (Mr. GRAHAM), and the Senator from Nebraska (Mr. SASSE).

Mr. DURBIN. I announce that the Senator from New Jersey (Mr. MENENDEZ), the Senator from Washington (Mrs. MURRAY), and the Senator from Hawaii (Mr. SCHATZ) are necessarily absent.

The PRESIDING OFFICER (Mr. BARRASSO). Are there any Senators in the Chamber wishing to vote or to change their vote?

The yeas and nays resulted—yeas 77, nays 17, as follows:

[Rollcall Vote No. 196 Leg.]

YEAS—77

Alexander	Franken	Murkowski
Ayotte	Gardner	Murphy
Baldwin	Gillibrand	Nelson
Bennet	Hatch	Perdue
Blumenthal	Heinrich	Peters
Booker	Heitkamp	Portman
Boozman	Heller	Reed
Boxer	Hirono	Reid
Brown	Hoeven	Rounds
Burr	Inhofe	Sanders
Cantwell	Isakson	Schumer
Capito	Johnson	Scott
Cardin	Kaine	Shaheen
Carper	King	Stabenow
Casey	Kirk	Sullivan
Cassidy	Klobuchar	Tester
Cochran	Lankford	Tillis
Coons	Leahy	Toomey
Corker	Lee	Udall
Cornyn	Manchin	Vitter
Cruz	Markey	Warner
Daines	McCain	Warren
Donnelly	McCaskill	Whitehouse
Durbin	McConnell	Wicker
Feinstein	Merkley	Wyden
Flake	Mikulski	

NAYS—17

Barrasso	Ernst	Roberts
Blunt	Fischer	Rubio
Coats	Grassley	Sessions
Collins	Moran	Shelby
Cotton	Paul	Thune
Crapo	Risch	

NOT VOTING—6

Enzi	Menendez	Sasse
Graham	Murray	Schatz

The PRESIDING OFFICER. On this vote, the yeas are 77, the nays are 17.

Three-fifths of the Senators duly chosen and sworn having voted in the affirmative, upon reconsideration, the motion is agreed to.

The Senator from Kentucky.

Mr. PAUL. Mr. President, could we have order?

The PRESIDING OFFICER. The Senate will be in order.

Mr. PAUL. Will the Chair inform me when I have 5 minutes remaining?

The PRESIDING OFFICER. The Senator will be so notified.

Mr. PAUL. Mr. President, tonight begins the process of ending bulk collection. The bill will ultimately pass. We always look for silver linings. I think the bill may be replacing one form of bulk collection with another, but the government, after this bill passes, will no longer collect our phone records. My concern is that the phone companies still may do the same thing. Currently, my understanding is the NSA is at the phone company sucking up the phone records and sending them to Utah. My concern is——

The PRESIDING OFFICER. Order in the Senate, please. The Senator deserves to be heard.

Mr. PAUL. My concern is that under the new program, the records will still be sucked up into NSA computers, but the computers will be at the phone company, not in Utah. So the question is, Will it be a distinction without a difference? The question also will be, Will this be individualized?

One of the issues about the Fourth Amendment that was the biggest part of the Fourth Amendment for our Founding Fathers was that a warrant should be individualized. General warrants were what we fought the Revolution over. James Otis fought a famous case in the 1760s, and he fought against the British soldiers writing their own warrants.

What is interesting is that part of the PATRIOT Act allows our police to write their own warrants. We have something called national security letters. These have been done by the hundreds of thousands. Interestingly, when the President was in the Senate, he was opposed to national security letters and said that they should have judicial warrants. Now, it is interesting that in this bill that will pass, it is supported by the President, supported by the Director of National Intelligence, and now supported in a wide bipartisan fashion.

It concerns me whether or not——

The PRESIDING OFFICER. The Senate will be in order.

Will the Senator please suspend.

The Senate will be in order. Please take your conversations out of the well, out of the Chamber. The Senator deserves to be heard.

Mr. PAUL. It concerns me that the President, who supports the bulk data collection and has been performing it illegally for 6 years, now supports this bill. The devil is in the details.

The question is, Will the new bill still allow bulk collection by the phone companies? Will they be able to put into the search engine not an individual about whom we have suspicion but an entire corporation? This is what was revealed when we saw the warrant that had Tsarnaev's name on it.

The Director of National Intelligence came before the American people, came before Congress and swore under oath that they weren't doing this. Part of my problem with the intelligence-gathering in our country is it is hard for me to have trust. It is hard for me to have trust in the people to whom we are giving great power.

They also insist we won't be able to catch terrorists. They insist the bulk collection allowed them to catch terrorists. But then it turned out, when it was investigated, when we looked at the classified documents, when the President's bipartisan privacy and civil liberties commission looked at this, when his review board looked at this, and then when the Department of Justice inspector general looked at this,

they all found that there was no unique data, there was no great discovery, there was no great breaking up of a terrorist ring.

People have brought up the Boston Bomber, the Tsarnaev boy. They say: Well, we need this. We need the PATRIOT Act after the bombing to get his phone records.

That is the most absurd thing I have ever heard. He has already committed a bombing. In fact, I think he was dead at that point, and they are saying we couldn't get a warrant to look at his phone records? It is absolutely absurd.

I had a meeting with somebody from the intelligence community about 6 months ago, and I asked them this question: How do we get more information about terrorists—with a warrant with their name on it, where we can go as deep into the details as we want, or this metadata collection that uses a less-than-constitutional standard? And he said: Without question, we get more information with a warrant than we do through the metadata.

When someone commits an act of atrocity, there is no question we would get a warrant, but I would go even further. I would say that I want to get more warrants on people before they blow up things. I would say that we need more money spent on FBI agents analyzing data and trying to find out whom we have suspicion about so we can investigate their records. I think we spend so much money on people about whom there is no suspicion that we don't have enough time and money left to go after the people who would actually harm us.

The people who argue that the world will end at midnight tonight——

The PRESIDING OFFICER. The Senator will please suspend.

Order in the Chamber. Please take your conversations off the floor.

Mr. PAUL. The people who argue that the world will end and that we will be overrun by jihadists tonight are trying to use fear. They want to take just a little bit of our liberty, but they get it by making us afraid. They want us to fear and give up our liberty. They tell us that if we have nothing to hide, we have nothing to fear. That is a far cry from the standard we were founded upon—innocent until proven guilty.

One of the objections I tried to bring forward earlier but was interrupted repeatedly was that the PATRIOT Act was originally intended to go after foreigners and terrorists. We allowed a less-than-constitutional standard. We didn't ask for probable cause; we just said it had to be relevant, the information had to be relevant to an investigation about terrorists. But here is the problem, and this is one of the big problems I have with the PATRIOT Act.

We now use parts of the PATRIOT Act to arrest people for domestic crime. Section 213, sneak-and-peek, where the government can come into your house, place listening devices, never announce they were ever in your house, and then leave and monitor your behavior and never let you know they were there, is being used 99.5 percent of the time for domestic crime.

So, little by little, we have allowed our freedom to slip away. We allowed the Fourth Amendment to be diminished. We allowed the narrowing loss of something called probable cause.

People say: Well, how would we get terrorists with that?

The vast majority of warrants are approved in our country—the vast majority of warrants that are Fourth Amendment warrants where we individualized and put a name on it and asked probable cause. If tonight the police are looking for a rapist or a murderer, they will go to the house, and if they suspect the person is inside but nothing is imminently happening, they will stand on the curb and they almost always get a warrant.

Do you think there is a judge in this land who would not grant a warrant—particularly after the Boston bombing—to look at the Tsarnaev brothers' records? There is not a judge in the land who would say no. I would venture to say that in advance there is not much chance that a judge would say no if you went to them and said: The Russians have given us indication and evidence that he has been radicalized and has associated overseas with people who are training to attack us.

There is no reason why the Constitution can't be used. But we just have to not let those who are in power make us cower in fear. They use fear to take your freedom, and we have to be very, very careful of this.

Now, some are saying I am misrepresenting this, that I am saying the government is listening to your phone calls. I am saying they are collecting your phone records. There are programs, though, in which there may be looking at content—emails, for example. The current law says that after 6 months even the content of your email has no protection. We have a very good piece of legislation to try to fix that. But realize that those who are loud, those who are really wanting you to give up your freedom, don't believe the Fourth Amendment protects your records at all.

And this is a big debate. We went to the court. The Second Circuit Court of Appeals—the highest court in the land just below the Supreme Court—said that what they are doing is illegal, but we don't yet have a ruling on whether it is constitutional.

One of my fears about the bill we are going to pass—the sort of in-between step some think may be better—is that it could moot the case. This means the court case will never get heard by the Supreme Court. I have a court case against the NSA. There is another district court that has ruled against the NSA. We now have an appellate ruling against the NSA. The court may well look at the activity of the Senate and say: Well, you guys have fixed the problem. We don't need to look at it anymore. It is no longer relevant.

My other concern about this new bill that is going to pass is that the same people will judge it who judged the previous system. These people are called the rubberstamp courtroom, also known as FISA. Realize that the FISA Court is the court that said the collection of all Americans' records is relevant. The appellate court basically laughed at this notion and said that it sort of destroys any meaning to the word ''relevant'' if you collect everybody's records. It is not even a modifier. Instead of saying ''relevant,'' they should have said ''You can have everyone's records all the time.''

One of my other concerns about the in-between solution we are going to choose is that some are conjecturing—and you have to be suspicious of a government that often lies about their purpose—some are conjecturing that they are going to collect more phone data under the new system. One of the complaints last week, as there was discussion about this—in the newspaper, it was reported that really they were only collecting about 20 to 30 percent of your cell phone data. They were trying to collect all of your land line data, but they weren't for some reason collecting all of your cell phone data. One of my concerns is that as we go to this new system, they may actually be better at collecting our phone records and they may well be able to collect all of our cell phone data.

Unless we go to a system where we individualize the warrants, unless we go to a system where a person's name is on the warrant, I am going to be very, very concerned.

Now, we will present amendments on this bill. We tried to negotiate to be allowed to present amendments, but there wasn't a lot of negotiating that went on in the last week—in fact, there was none. We will still try. We will put amendments forward, and we will try to get amendments to make the bulk collection less bad when it does occur. One of the things we would like to do is to say that when they search the phone records, they can't put the name of a corporation in there; they would have to put in an individual's name.

It is kind of tricky, the way these things are worded. The wording of this bill will say they can only put a U.S. person into the selector term to search all phone records. The problem is that they define ''U.S. person'' as also meaning corporation or association or grouping. So there is a little bit of looseness to the language. So if we are still going to allow corporations, what is to stop them from going back and putting AT&T or Verizon in the selection? Once again they will be looking at all the phone records, and all we will have done is transferred the phone records from government control in Utah to phone company control in another location. Will we be trading bulk collection in Utah for bulk collection under the phone companies?

There are good people who believe this bill will reform, and I think they

are well-intended. I think they are good people who really think that we will end bulk collection and that it won't happen. My fear, though, is of the people who interpret this work at a place known as the rubberstamp factory over at FISA. It is a secret court, and it is a court in which 99.5 percent of the time they approve warrants. Warrants are simply rubberstamped over there. In fact, they approved that ''relevant'' meant all of your records. So my question is, If they put AT&T as a selector item, will we have the same thing, just in a different location?

I have several amendments I am interested in if we are able to amend the bill.

One is that the search would have to be an individual. That is more consistent with the Fourth Amendment.

Another one would change the standard to the constitutional standard, which would be that there would have to be probable cause, which is a higher standard than simply saying it is relevant. Then we would actually be sending a new signal to the FISA Court.

Another amendment I have, which I think would go a long way toward making the PATRIOT Act less bad—I think is the best way to put it—would be to say that any information gathered under a less-than-constitutional standard could only be used for foreigners and terrorists. See, that was the promise. At the time, there were people who opposed the PATRIOT Act—not enough, but there were a few—and when they opposed the PATRIOT Act, they said their fear was that it would be used against American citizens.

They said: No, no, we are only going after terrorists. But the law allows them to do it, and we now have sections of the PATRIOT Act which 99.5 percent of the time are being used for domestic crime. We have also seen that the Drug Enforcement Agency—it is alleged—is using information gathered under the PATRIOT Act to then go back and recreate cases against people for domestic crime.

The question we have to ask ourselves is, Are we so frightened that we are willing to give up our freedom? Are we really willing to trade liberty for security?

I think the U.S. Court of Appeals had some great points that they made when they ruled against the government, and I think what is important to know is that the President has continued to do this illegally. You have seen him on television. The President has been saying: Well, Congress is just getting in the way. If Congress would just do their job and get rid of this, everything would be OK. But the truth is that Congress never authorized this. Even the authors of the PATRIOT Act said this was not something Congress ever even contemplated. The court is now saying that as well. This was done by the executive branch—admittedly, both a Republican executive branch and a Democratic executive branch—but this wasn't created by Congress.

So when the President says ''Well, Congress should just do this,'' the question that has never been asked by anyone in the media is ''Why doesn't he stop it?'' Everybody who has given advice has said he would, and he will come out and say he believes in a balanced solution, but he really is just abdicating the solution and has never discontinued the program, even when he has been told explicitly by the court that the program is an illegal program.

This is what the U.S. court of appeals said in the case ACLU v. Clapper:

> We agree with the appellants that such an expansive concept of ''relevance'' is unprecedented and unwarranted. . . . The records demanded are not those of suspects under investigation, or of people or businesses that have contact with such subjects, or of people or businesses that have contact with others who are in contact with the subjects.

So even two steps removed, we are gathering records that are completely irrelevant to the investigation. We are gathering up the phone records of innocent Americans.

The other side will say: Well, we are not looking at them.

So I have been thinking about this. Our Founders objected to the British soldiers writing warrants. They objected to them coming into their house and grabbing their papers. Do you think our Framers would have been happy if the British Government said: OK, we are just breaking your door down, we are just getting your papers, but we are not going to look at them. Do you think that would have changed the mindset of the Framers? So the fact that they say they are not looking at our records—is that any comfort or should it be any comfort? The act of violation is in taking your records. The act of violation is in allowing the police or a form of the police—the FBI—to write warrants that are not signed by a judge.

The court goes on to say: ''The interpretation that the government asks us to adopt defies any limiting principle.'' The idea of a limiting principle when the court looks at things is that, the way I see it, is the difference between something being arbitrary, where there is no sort of principle that confines what would happen—if you have a law that has no limiting principle, it is essentially arbitrary.

This is what Hayek wrote about in ''The Road to Serfdom.'' Hayek talked about the difference between the rule of law and having an arbitrary interpretation of the law.

The danger of having an arbitrary interpretation of the law and the danger of having general warrants is that they have been used in the past with bias. People have brought their own bias into this. In the sixties, the bias was against civil rights activists and against Vietnam war activists. In the forties, the bias was in incarcerating and interring Japanese Americans. But what was consistent in all of these circumstances was that there was a generalization—a generalization based on the color of your skin, whether you were Asian American or African American, and also about the shade of your ideology. There is a danger in allowing the government to generalize without suspicion and to disobey the Fourth Amendment, and the danger comes that the government could one day generalize and bias could enter into things.

We have on our records right now laws that allow an American citizen to be detained. It is not specifically a part of the PATRIOT Act, but it is along the same lines as this, that you are getting rid of the due process amendments and the ability of the Bill of Rights to protect an individual. When we allow an individual to be detained without a trial, what happens is that there is the possibility that someone could decide we don't like ''those'' people. And when you say that could never happen, think about the times in our history when it has.

Richard Jewell, everybody said he was the Olympic Bomber. He was convicted on TV. Within hours, people said: Richard Jewell is guilty. Think about if he had been a Black man in 1920 in the South what may have happened to him. Think about the possibility for bias entering into our government. Think about what Madison said about government is—Madison said that we restrain government because we are worried that government may not be comprised of angels. If government were comprised of angels, we would not have to worry about restraining government.

Patrick Henry said that the Constitution was about restraining government, not the people. It is not enough for people to say: Oh, I am a good man or I am a good person or the NSA would never do this. The other problem that makes us doubtful is that the NSA has not been honest with us. If they want to develop trust again, the President should have immediately let the person who lied to us go, the Director of National Intelligence.

The appeals court concluded by saying that the government's bulk collection of telephone metadata exceeds the scope of what Congress has authorized and therefore violates section 215 of the PATRIOT Act. Some will try to argue that this debate was not worth the time we took on it. I could not disagree more. I am like everybody else. You know, I prize my time with my family and being at home on the weekends. I wish we would have done this in a more sensitive way, where we would have had more time and had an open amendment process.

But we waited until the end. We waited until the final deadline. This is a characteristic of government. It is a flaw in government, frankly. We lurch from deadline to deadline. People wonder why Congress is so unpopular. It is because we go from deadline to deadline and then it is: Hurry up. We have no time to debate. We just must pass it as is.

The biggest debate against amendments is—and it finally convinced people who did not like this. They so much dislike amendments and slowing down the process, they are just going to take it. Even though they don't like it, they are going to pass what the House passed. It is unlikely any amendments will pass.

But the thing is, we need to get away from lurching from deadline to deadline. What happens, with budget or spending or any of these bills, is we are presented with thousand-page bills with only hours to go. About a year ago this came up. At that time, we were presented with a 1,000-page bill with 2 hours to go. I read the Senate rules. It said: We are supposed to be presented with the bill for 48 hours in advance.

So I raised my hand and made a motion. The motion I made was: Guys, we are breaking the rules here. Men and women, we are breaking the rules here. So they just voted to amend the rules for that bill and ignore the rules. This is why the American people are so frustrated. People here in town think I am making a huge mistake. Some of them, I think, secretly want there to be an attack on the United States so they can blame it on me. One of the people in the media the other day came up to me and said: Oh, when there is a great attack, are you going to feel guilty that you caused this great attack?

The people who attack us are responsible for attacks on us. Do we blame the police chief for the attack by the Boston Bombers? The thing is, is that there can be attacks even if we use the Constitution. But there have been attacks while collecting your bulk data. So the ones who say: Well, when an attack occurs, it is going to be all your fault, are any of them willing to accept the blame? We have bulk collection now. Are any of them willing to accept the blame for the Boston bombing, for the recent shooting in Garland?

No, but they will be the first to point fingers and say: Oh, yes, it is all your fault. We never should have given up on this great program. I am completely convinced that we can obey the Constitution, use the Fourth Amendment as intended, spirited letter of the law, and catch terrorists. When we look objectively at this program, when they analyzed the classified information, they found that there was no unique data. We had to fight them tooth and nail because they started out saying that 52 cases were cracked by the bulk data program.

But then when the President's own bipartisan commission looked at it, it turned out that none of that was true. This gets back to the trust issue. If we are going to be lied to by the Director of National Intelligence, it is hard for us to believe them when they come forward and they say: Oh, this is protecting us. We have to have it. But what we are hearing is information from someone who really did not think it was a big deal to lie to us about whether the program even existed.

Mark my words, the battle is not over. There are some—and I talked with one of the, I would say, smarter people in Silicon Valley, somebody who knows this from an intimate level, how things work, and how the codes and programs work.

He maintains that the bulk collection of phone data is the tip of the iceberg, that there is more information in other data pools that are classified. Some of this is done through an Executive order called 12333. I am not sure I know everything in it. I have had no briefings on it. So anything I will tell you is from the newspaper alone. But the thing is, is that I would like to know: Are we also collecting your credit card information? Are we collecting your texts? Are we collecting your emails?

They have already told us the Fourth Amendment does not protect your emails, even the content, after 6 months. In fact, really they have told you, the Fourth Amendment does not apply to your records at all. So be very careful about the people who say: Trust us. We will never violate your freedom. We will never take advantage of things. The President's Privacy and Civil Liberties Oversight Board's conclusion was that:

> Section 215 of the PATRIOT Act has shown minimal value in safeguarding the Nation from terrorism. We have not identified any single instance involving a threat to the United States in which the program made a concrete difference in the outcome.

The President's privacy board went on to say:

> The government's collection of a person's entire telephone calling history has a significant and detrimental effect on individual privacy.

When they talked about whether the phone records were relevant to an investigation, the President's Commission said this:

> First, the telephone records acquired under the program have no connection to any specific FBI investigation at the time of their collection. Second, because the records are collected in bulk, potentially encompassing all telephone calling records across the Nation, they cannot be regarded as relevant to any FBI investigation.

Here is the continuing danger to us, though: It is, I think, maybe a minor success that we are going to prevent the government from collecting these records. But realize that the interpretation of this will still occur in secret in the FISA Court. This is the FISA Court that said that collecting everyone's records was relevant.

It completely destroys the notion that the word ''relevant'' has any meaning at all. This will be the question: Whether we can trust the FISA Court to make an interpretation that is at a higher degree of discernment than the one in which they said ''relevant'' can mean anything. The original USA FREEDOM Act, as passed originally by the House committee, was a better bill. It was gradually watered down until even the Director of National Intelligence, the one who lied about the program, now supports it, which gives me some misgivings.

But the records that will be collected—the question is, How will we have an interpretation by the FISA Court? The original bill had an advocate. I thought this was a good part of the original bill. There would be a judicial advocate who would argue on the side of those who were having their records taken. So there would be an adversarial court, lawyers on both sides.

Many people who write about jurisprudence and trying to find justice say that one of the essential functions of a court system, in order to find justice, is that there has to be a lawyer on both sides. There has to be an advocate on both sides. The truth is not always easy to find. The truth is presentation of facts by one side, presentation of contrary facts by the other side, and someone has to figure out which facts are more believable or which facts trump other facts.

So I think a judicial advocate would have been good. They are still going to have it. They call it by a different name now, but it will be optional at the discretion of the FISA Court. So the court that ruled that all of your records are relevant now will have a choice as to whether to give you an advocate. That does not give me a great deal of comfort.

There are other ways we could do this. We occasionally do look at terrorism cases in regular Federal court. When names come up that could jeopardize someone's safety at our intelligence agency or a secret, Federal courts can go into secret session. I have heard the Senator from Oregon often mention this. I think it is a great point that no one wants to reveal the names of anyone or the code or the secrets of how we do this. But if we are talking about constitutional principles, we want to do it in the open. Laws should not be discussed in secret.

As we move forward, the PATRIOT Act will expire tonight. It will only be temporary. They will ultimately get their way. But I think the majority of the American people actually do believe the government has gone too far. In Washington, it is the opposite, but I think Washington is out of touch. There will be 80 votes, you know, to say: Continue the PATRIOT Act—maybe more.

But if you go into the general public, if you get outside the beltway and visit America, you find it is completely the opposite. There was a poll a couple of weeks ago that said: Over 80 percent of people under age 40—over 80 percent of them—think that the government collecting your phone records is wrong and should not occur. So I think really this will be useful. People say: You are destroying yourself. You should have never done this. The American people will not side with you.

People wished me harm and wished that this would be unsuccessful. But you know what, I came here to defend the Bill of Rights and to defend the

Constitution, popular or not. But I frankly think that the Bill of Rights and the Constitution are very popular, very important, and I will continue, as long as I have breath and as long as I am here to defend them.

I yield back the remainder of my time.

The PRESIDING OFFICER. The Senator from Oregon.

Mr. WYDEN. Mr. President, before he leaves the floor, I just want to make sure, having worked with Senator PAUL for many, many months now, that I especially appreciate his efforts in the last few days in this week to try to accommodate this body with respect to amendments. My colleague has said repeatedly that he was very interested in a short list of amendments, that he hoped to have some modest time that would be available for these amendments.

He and I have worked together on a number of them. I think it is a reflection, as people think about this debate and on a topic that is of such enormous importance, that my colleague from Kentucky, especially with respect to this amendment issue, has tried continually to be reasonable and to be accommodating to this body.

Until just a few hours ago, I was at home in Oregon having townhall meetings, flew all night to be here for this extremely important session. Of course, the topic we discussed this evening was front and center in terms of my constituents.

The message from Oregonians at these townhall meetings was very clear. The people whom I have the honor to represent in the Senate want policies that advance their security and protect their liberties. The program we have been talking about tonight in the Senate really does not deliver either. It does not make us safer. It chips away at our liberties.

I am going to spend a little bit of time this evening making the case for those kinds of arguments and laying out the challenge for the days ahead.

Now, with respect to this safety issue, all of us understand—particularly the Presiding Officer, who has been on the Intelligence Committee, as I have, for over 14 years—that it is a dangerous world. Anyone who serves on the Intelligence Committee knows that beyond any kind of debate.

So we want policies that really deliver both security and liberty. This is what the President's own experts had to say with respect to this program that involves collecting millions and millions of phone records on law-abiding Americans. This was a group that was appointed and spent a considerable amount of time looking at the bulk phone records collection program. They issued a report, and will I just paraphrase what is the central finding, on page 104 of their report: As to information contributed to terrorist investigations by the use of section 215 telephony metadata—that is the collecting all of these millions and millions of phone records—these experts say that ''could readily have been obtained in a timely manner using conventional Section 215 orders.''

Now, the reason that is important is it spells out and recognizes that those who signed this report are individuals with some of the most pristine antiterror credentials in this country—Mike Morell, for example, the former Acting Director of the CIA; Richard Clarke, who held an extremely important position in two administrations and served with both Republicans and Democrats. Both of them are signatories to this important report.

Beyond that—and it has not received much attention—the reality is that our government, on top of everything else, has emergency authorities so that when those who are charged with protecting our country believe there is a threat to the Nation, they are allowed to issue an emergency authorization to get the information they need right away, and then they can go back and get the warrant approved after the fact.

Nobody is talking about eliminating that emergency authority. So what we have is a program that the most authoritative antiterror experts in the country believe does not make our Nation any safer. I read the most significant finding in their report.

On top of that, as I just indicated, emergency authorities are still preserved. In fact, I have indicated to our President and to those who work in the intelligence agencies that if at any point the executive branch and, particularly, the intelligence agencies feel that their emergency authorities are inadequate to protect the country, I personally would be willing to support efforts to ensure that those emergency capabilities are reformed and our country can take the steps it needs when it is necessary.

On top of this question, with respect to the issue of our safety, I want to talk about what I heard at some length earlier today with respect to how the program worked. I heard a number of Senators say that nobody in government is listening to these calls. That was repeated a number of times on the floor of this body.

When the government, under this program, knows whom you called, when you called, and where you called from, in many instances the government doesn't need to be listening. If the government knows, under this program, that a person called a psychiatrist 3 times in 36 hours—twice after midnight—that is a lot of private and personal information. The government doesn't need to be listening to that call.

So as to this notion that some who have wanted to make sure that our country would have both security and liberty are saying that it is a fantasy that the government is listening to calls, I could tell you that those who have been trying to reform the program have said, in effect, that the government doesn't need to listen to those calls. If the government has that amount of private and personal information, the government knows a lot about you, and it really doesn't need to listen. Certainly, if you are talking about a land line, then the government knows where you are calling from if they have a phone book.

So with respect to this question of the government listening, I want it particularly understood that a program such as this, when the government has this kind of information, I believe, represents a threat to our liberty. The reason why I think so is that hardly a week goes by when databases aren't violated. No. 1, we see that reported regularly in the press. No. 2, we have known about unfortunate times in our history—J. Edgar Hoover comes to mind—when this kind of information could be used. And, No. 3, I have been very concerned, given what our former colleague, Senator UDALL, and I had to do with respect to bulk phone record collection of email. We battled to end this. Of course, this was email that could be read by government agencies. We battled with various intelligence leaders saying that we felt this was a violation of people's rights and it wasn't effective. They asserted for months and months that it was. Finally, one day they woke up and said the program wasn't needed any more.

None of this would have even happened had not Senator Udall and I made that case repeatedly. The intelligence leadership knew that we were not going to give it up, but that is what goes on if there isn't a check on some of these kinds of procedures.

Senator PAUL made mention of the fact that the intelligence leadership has not exactly been straight with the American people on these issues. I emphasize that we are not talking about the thousands and thousands of law-abiding patriotic, dedicated, wonderful people who work in the intelligence field. Day in and day out they do so much for our country. We are so appreciative of all they do. They are the ones who do the hard work, for example, to capture Bin Laden and day in and day out to make us safer. But the intelligence leadership, on the other hand, as noted by our colleague from Kentucky, has not always been straight with the American people. I spent many months trying to decipher what the former NSA Director meant when he said the government doesn't collect any dossiers on millions of Americans.

I pointed out I had been on the Intelligence Committee for a long time and I had never heard the term ''dossier'' used. So I tried to learn more about it, used private opportunities and public opportunities, and just couldn't get the information. So, finally, I said: I have to ask this question in public.

On the Intelligence Committee you don't get but perhaps 20 or 25 minutes a year to ask questions in public, to hold intelligence leaders accountable

on policy matters—not secret operations, because secret operations have to stay secret, but policy matters.

So, after being stonewalled for many months—many months—I finally said I have to ask this question in public. So to make sure no one would feel ambushed, I sent the question to the Director of National Intelligence, Mr. Clapper. I sent it a day ahead of time.

Then I didn't hear anything about its being inappropriate or in violation of classification rules. So I asked in public: Does the government collect any type of data at all on millions or hundreds of millions of Americans? I was told no, and that answer was obviously false. I tried to get it corrected, and we still couldn't get it corrected.

Of course, then Mr. Snowden spoke out publicly and pointed that out. Since that time, the Director of National Intelligence and his representatives have given these five different explanations for why that answer was given. So that is why you have to ask the hard questions. You have to ask the hard questions about these issues.

I see my friend and colleague Senator HEINRICH has joined us tonight. I am so pleased that he has joined the Intelligence Committee. Senator HEINRICH is one of those Senators who subscribes to that view that I just mentioned—that it is our job to ask the hard questions. It may be uncomfortable. It is not designed in any way to convey disrespect. We see it as our job to ask the hard questions.

I would be interested in my colleague's thoughts with respect to this issue and to have him be given a chance to participate in this colloquy.

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

Mr. HEINRICH. First, I thank my friend from Oregon and I recognize the substantial leadership he has shown on this issue over the years. Long before I came to the Intelligence Committee and long before Edward Snowden began to steal documents, Senator WYDEN, along with Senator Mark Udall and others, were doing everything they could—without disclosing classified information—to shine a light on the fact that the U.S. Government was collecting massive volumes of data on millions of law-abiding American citizens. My friend from Oregon deserves our thanks for that leadership.

Now, after the bulk call data collection program was revealed to the public, the government, frankly, defended it and defended it vigorously. It took a number of months for the intelligence community and the rest of the administration to take a deep breath and really assess whether bulk metadata collection was necessary, whether it was effective, and to consider whether there were other less intrusive, more constitutionally grounded ways to accomplish these same goals.

Starting with the President's Review Group on Intelligence and Communications Technologies, the administration began to agree that ''some of the authorities that were expanded or created in the aftermath of September 11 unduly sacrifice fundamental interests in individual liberty, personal privacy, and democratic governance.'' And they recommended changing those authorities in order to ''strike a better balance between the competing interests and providing for the common defense and securing 'the Blessings of Liberty to ourselves and our Posterity.' ''

Following that, multiple efforts have been made to update and reform FISA and to update and reform the USA PATRIOT Act. None of those have been successful. But now we are forced to come to a resolution through a combination of, frankly, procrastination, and, I think, misguided hope that the American people would look the other way while the government continued to vacuum up and store their personal information and data as part of a program that even the intelligence community acknowledges can be accomplished through less intrusive means.

I will be honest. The current USA FREEDOM Act isn't what I consider perfect. For example, I prefer that it include strong reform of section 702 collection, but I accept that circumstances require us to be pragmatic, require us to govern and move forward and to work with one another in both parties to find compromise. That is what the USA FREEDOM Act is. It is a product of bipartisan compromise.

That is why it passed the House of Representatives by a vote of 338 to 88. And let's be blunt, many of those who voted against it didn't do so because they support bulk collection. They did so because they want to see section 215 wither and die in its entirety. That is the political reality we face today, and we need to accept it rather than demanding a continuation of a program that the appeals court has determined is illegal.

Mr. WYDEN. I thank my colleague for his statements and would just want to explore this a little bit further. I hope that those who are following this debate understand that my colleague from New Mexico is a real rising star in the Senate. He and I would like the USA FREEDOM Act to go further, and we both worked together on legislation that would make additional reforms. Certainly, our colleagues on the Intelligence Committee and here in the Senate can expect to see us continuing to work together to advance these additional reforms over the coming months and years. For now, the two of us are saying we ought to support the USA FREEDOM Act and then move on—move on to other critical areas.

I particularly want to see closed what is called the backdoor search loophole, which my colleague from New Mexico talked about. What this means, colleagues, is that when you are engaged in a lawful search of someone who is a threat overseas, pursuant to section 702 of the Foreign Intelligence Surveillance Act, very often law-abiding Americans can get swept up in this search and have their emails looked at.

This is a problem today, and my view is it is likely to be a growing concern in the future because, increasingly, communications systems around the world are becoming globally integrated, so the amount of emails that are reviewed of Americans is likely to grow. But we can't get that change here tonight. So, as my colleague from New Mexico has mentioned, the USA FREEDOM Act would make several worthwhile reforms, such as increasing transparency, reducing the government's reliance on secret laws. But from my perspective, the centerpiece of it is ending the bulk collection of Americans' information under the PATRIOT Act.

I have been trying to close this particular loophole for close to a decade now. Some of our colleagues have said the bulk collection has never been abused; that no one's rights have been violated. My own view is—and I will ask what my colleague thinks—that vacuuming up all this information, particularly when databases get violated all the time—we have seen historically instances where there has been improper conduct by the government. I believe dragnet surveillance violates the rights of millions of our people every day.

Vacuuming up the private phone records of millions of Americans with no connection to wrongdoing is simply a violation of their rights.

And vacuuming up Americans' email records, which I pointed out before my colleague came to the floor—which he and our former colleague Senator Udall and I battled—is surely a violation of the rights of Americans as well. Colleagues, that wouldn't have been pointed out at all—it wouldn't have been pointed out at all—unless Senator Udall and I, with the help of our friend from New Mexico, hadn't been pushing back on it. Finally, one day the government said: Well, we will get rid of it because it wasn't effective. They got rid of it because they saw they were going to get hard questions, the kinds of questions my friend from New Mexico has been asking.

Now, with respect to the legality of this program, I know my colleague and I actually filed a legal brief, along with our former colleague Mark Udall, when the Court of Appeals for the Second Circuit was examining that program. In our brief, it was argued that we were able to debunk many of the claims that had been made about the effectiveness of the program.

I think it would be helpful if my colleague from New Mexico laid out some of that analysis here tonight. I would ask the Senator from New Mexico to begin, and I would encourage him to start by addressing the claim that the bulk collection of Americans' phone records is essential for stopping terrorist attacks. My question to my colleague is, Is there any evidence, any

real concrete evidence, to support that claim?

Mr. HEINRICH. I thank my friend from Oregon and begin by saying that despite what we may have heard from talking heads on the Sunday shows and on the cable news networks, the answer is no. There is simply no evidence to support those claims.

When this mass surveillance was first revealed to the public 2 years ago, the executive branch initially responded to questions like this by claiming that various post-9/11 authorities had resulted in the thwarting of approximately ''54 terrorist events in the U.S. homeland and abroad.''

Now, a number of us, including my friend from Oregon and my former colleague from Colorado, Senator Udall, began to pull on that thread to really parse down and see just what the executive branch was talking about. First, of those 54 terrorist events, it turned out that only 13 were actually focused in the United States. But more importantly, those numbers conflated multiple different programs, including authorities under section 215 and different authorities under section 702.

On June 19, 2013, my colleague from Oregon and Senator Udall pointed out that ''it appears that the bulk phone records collection program under section 215 of the USA PATRIOT Act played little or no role in most of these disruptions. Saying that 'these programs' have disrupted 'dozens of potential terrorist plots' is misleading if the bulk phone records collection program is actually providing little or no unique value.''

Of the original 54 instances the executive branch pointed to, every one of them crumbled under scrutiny. None of them actually justified the continued existence of the bulk collection program.

Let me take a moment, with the indulgence of our colleagues, and read what was written by Judge Leon of the District Court for the District of Columbia, when he ruled in the Klayman v. Obama case. This is a little long, but I think it is important this be part of the official record of this debate.

Judge Leon writes:

> [T]he Government does not cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature. In fact, none of the three ''recent episodes'' cited by the Government that supposedly ''illustrate the role that telephony metadata analysis can play in preventing and protecting against terrorist attack'' involved any apparent urgency.

He continues to write that:

> []In the first example, the FBI learned of a terrorist plot still ''in its early stages'' and investigated that plot before turning to the metadata ''to ensure that all potential connections were identified.'' []Assistant Director Holley does not say that the metadata revealed any new information—much less time-sensitive information—that had not already come to light in the investigation up to that point.

The judge continues:

> []In the second example, it appears that the metadata analysis was used only after the terrorist was arrested ''to establish [his] foreign ties and put them in context with his U.S. based planning efforts.'' []And in the third, the metadata analysis ''revealed a previously unknown number for [a] co-conspirator . . . and corroborated his connection to [the target of the investigation] as well as to other U.S.-based extremists.''

Continuing to quote Judge Leon:

> []Again, there is no indication that these revelations were immediately useful or that they prevented an impending attack. Assistant Director Holley even concedes that bulk metadata analysis only ''sometimes provides information earlier than the FBI's other investigative methods and techniques.''

Finally, Judge Leon writes:

> []Given the limited record before me at this point in the litigation—most notably, the utter lack of evidence that a terrorist attack has ever been prevented because of searching the NSA database was faster than other investigative tactics—I have serious doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism.

That is where the judge leaves off. And I will turn back to the Senator from Oregon to address the three cases we discussed in more detail in our amicus brief to the Second Circuit.

Mr. WYDEN. I thank my colleague. The first of these examples—and they really are kind of overblown examples about the effectiveness of bulk collection—is the case of an individual named Najibullah Zazi. Mr. Zazi was a known terrorism suspect, and a number of people have suggested that bulk phone records collection was somehow essential to stopping him because a query of the bulk phone records database for numbers linked to Mr. Zazi returned a previously unknown number belonging to another terrorism suspect.

However, since the government had already identified Zazi as a terrorism suspect prior to querying the bulk phone records database, it had all the evidence it needed to obtain the phone records of Zazi and his associates using an individualized section 215 order or other legal authorities.

In the second case, some have pointed to Mr. Moalin, the San Diego man convicted of sending $8,500 to support al-Shabaab in Somalia. The intelligence community has indicated that information from the bulk phone records database ''established a connection between a phone number known to be used by an extremist overseas . . . and an unknown San Diego-based number'' that belonged to Mr. Moalin. Yet there are ample existing authorities under which the United States can conduct surveillance on a phone number known to be used by extremists overseas and other phone numbers in contact with that phone number.

The argument that Mr. Moalin's case is an example of a unique value of bulk phone records collection is just not accurate. My view is this is yet another case that offers a misleading exaggeration with respect to the effectiveness of bulk phone records collection.

Finally, several supporters of the bulk metadata program have claimed that ''[i]f we had had [the bulk phone-records] program in place at the time [of the September 11, 2001 attacks,] we would have been able to identify'' the phone number of one of the hijackers, Khalid al-Mihdhar.

Just as in these other cases, however, the record indicates that Mr. Mihdhar's phone number could also have been obtained by the government using a variety of alternate means. Before September 11, the government was surveilling a safe house in Yemen but failed to realize that Mr. Mihdhar, who was in contact with the safe house, was actually inside the United States. The government could have used any number of authorities to determine whether anyone in our country was in contact with the safe house it was already targeting. It didn't need a record of every Americans' phone calls to establish that simple connection.

Mr. HEINRICH. I wish to expound on that point a bit, about the many other ways the government can legitimately acquire phone records of terrorism suspects, because I think this is a very important point to understand the tools that already exist that have been very effective and have proven themselves over time.

There are actually a number of legal authorities that can get the same information without the government collecting billions of call records—billions of call records that, in large part, belong to innocent Americans.

For example, the Stored Communications Act permits the government to obtain precisely the same call records that are now acquired through bulk collection under section 215 when they are ''relevant and material to an ongoing criminal investigation.''

Additionally, national security letters, which I point out do not require a court order, can also be used by the government to obtain call records for intelligence purposes.

Further, the government can also acquire telephony metadata on a real-time basis by obtaining orders from either regular Federal courts or the FISC for the installation of pen registers or trap-and-trace devices.

Finally, individualized orders for phone records, as opposed to orders authorizing broad bulk collection, can also be obtained under section 215.

I think those of us early in this debate thought that was what was going to occur under the PATRIOT Act in the first place. But that is what the USA FREEDOM Act seeks to require while prohibiting the bulk collection of millions of personal records. It even includes emergency authorization authority for the government to get records prior to getting court approval, subject to later court approval, in an emergency.

The government can use any of these authorities without any more evidence

than what is currently required to use the bulk phone records database, with less impact, I would point out, on the privacy interests of millions of innocent Americans.

I think at this point the Senator from Oregon and I have laid out our case as to why this dragnet bulk surveillance program fails to make our country measurably safer and why it should end. I am pleased to say that a number of people have finally come around to our way of thinking on this.

Mr. WYDEN. I thank my colleague. I will wrap up and then give the last word to my friend from New Mexico on the subject. He is absolutely right that some of the most authoritative leaders in our country—experts on terror—have reached the same judgment we have. I made mention of the President's Review Group on Intelligence and Communications Technologies, and I really would encourage colleagues who are following this debate and citizens across the country—that report is available online, and it is available in our office. Page 104 of that report is very explicit. It says that the information that would otherwise be obtained in collecting all of these phone records—millions of phone records of law-abiding Americans, people such as Mike Morell, former Acting Director of the CIA, and Richard Clark, who served in two administrations—they said it could have been obtained through conventional processes.

This is a program that is not making us safer. And it is not my judgment that ought to be the last word; it should be that of people like those I just quoted.

The Privacy and Civil Liberties Oversight Board's report on the telephone records program said pretty much the same thing:

> [T]he Section 215 program has shown minimal value in safeguarding the nation from terrorism. Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation.

I will close by way of saying—and I touched on this before my friend from New Mexico arrived—I would like to do a lot more than I believe is likely to happen here quickly in the Senate. I do want to see us finally throw in the dustbin of history this bulk phone records collection program because it doesn't make us safer and it compromises our liberty. But, as I indicated to my friend from New Mexico, I would also like to close this backdoor search loophole in the FISA Act, which is going to be a bigger problem in the days ahead given the evolution of communications systems and how they have become globally integrated.

I will close by saying that one of the most important issues we are going to have to tackle in the days ahead is going to deal with encryption. Encryption, of course, is the encoding of data and messages so that they cannot be easily read. The reason this will be an enormously important issue—and my colleague and I have talked about this—is because of the NSA overreach, the collection of all these phone records of law-abiding people. A lot of our most innovative, cutting-edge companies have found their customers raising real questions about whether their products can be used safely, and a lot of the purchasers who buy their products around the world are saying: Maybe we shouldn't trust them. Maybe we should try to start taking control over their servers and have local storage requirements and that sort of thing. So what our companies did, because they saw the effect of the overreach by the NSA, was they started to use encryption to protect the data and messages of the consumers who buy their products.

Most recently, the head of the FBI, Mr. Comey, rather than try to come back with a solution that protected both our privacy and our security, he said he was interested in requiring companies to build weaknesses into their products. Just think about that—requiring companies to build weaknesses into their products. So the government—which, in effect, caused this problem with the overreach—in effect, rather than trying to find a solution that worked for both security and liberty, said: We will start talking about requiring companies to actually build weaknesses into their products.

I and others have pointed out that once you do that, hang on to your hat. When the good guys have the keys, that is one thing, but when companies are required to build weaknesses into their products, the bad guys are going to get the keys in a hurry, too. And with all the cyber hacking and the risks we already have, we ought to be really careful about going where Mr. Comey, our FBI Director, has proposed to go.

But that is not for tonight. Tonight is not an occasion where we will be able to, on a bipartisan basis, close the backdoor-search loophole or where we will be able to come up with a sensible policy with respect to encryption rather than requiring companies to actually build weaknesses in their products. We will not be able to do that tonight. But we will now have a chance here in the Senate to take steps that have been bipartisan both here in the Senate and in the other body, in the House of Representatives, to end the bulk phone records collection program because it doesn't make us safer and it threatens our liberties.

I always like to close by thinking about Ben Franklin, who said that anybody who gives up their liberty to have security really doesn't deserve either.

I am so pleased to have a chance to serve with my colleague from New Mexico on the Intelligence Committee, who is going to be a thoughtful advocate for these kinds of policies, in my view, for many years to come. I thank him for his involvement tonight and would be happy to give him the last word of our colloquy at this time.

I yield to my colleague.

Mr. HEINRICH. I thank my friend from Oregon. I think he could not have chosen a more appropriate way to end than to reference what Ben Franklin said so many years ago, that great quote that ''those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.''

While many reforms still lie in front of us, I think, as we move forward to approving the USA FREEDOM Act, we move a lot closer to the balance that Ben Franklin articulated so well over 200 years ago. I look forward to working with my colleague from Oregon and all of our colleagues in achieving that balance and standing up for our constituents.

Mr. WYDEN. Mr. President, I yield the floor.

Mr. LEAHY. Mr. President, we did not have to end up here, just hours away from the midnight expiration of three surveillance authorities, and having just moved to proceed to the USA FREEDOM Act.

I have tried since last year to move legislation through the Senate to address these sunsets. In November, Senator REID brought the USA FREEDOM Act to the floor but the Republican leadership of the Senate blocked debate on it. When they took over the Senate, they assured us that they would send bills—including this one—through appropriate committee process. There were promises that the new leadership would not fill the amendment tree, and would use a transparent legislative process. But not one of those promises has been fulfilled with respect to any legislation dealing with the upcoming sunsets.

Once again this year, I proposed with Senator LEE a new version of the USA FREEDOM Act. That bill had significant process in the House, where it passed by an overwhelming margin earlier this month. And once again, the bipartisan coalition here in the Senate tried to get the bill passed. Two Fridays ago, the Senate Republican leadership did not allow us to debate the bill.

Tonight, the Senate did the right thing by invoking cloture on the motion to proceed to the USA FREEDOM Act. I am glad to see several Republicans switched their votes. This is significant progress, but it is late in coming.

We should have proceeded to this bill two Fridays ago. Had we done so, we could have stayed here to do our work, considered amendments, and passed the bill well in advance of tonight's sunset. Instead, we are hours away from expiration and just now considering legislation that many of us have been working on for years. Our intelligence community needs predictability and certainty, not a manufactured crisis.

If all Senators cooperate, we can finish this bill tonight. We can consider a

handful of amendments under a time agreement, and pass this bill before midnight. That would be the responsible thing to do.

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

The PRESIDING OFFICER (Mrs. CAPITO). Without objection, it is so ordered.

Mr. MCCONNELL. Madam President, I know of no further debate on the motion.

The PRESIDING OFFICER. The question is on agreeing to the motion to proceed.

The motion was agreed to.

USA FREEDOM ACT OF 2015

The PRESIDING OFFICER. The clerk will report the bill by title.

The legislative clerk read as follows:

A bill (H.R. 2048) to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes.

AMENDMENT NO. 1449

(Purpose: In the nature of a substitute)

Mr. MCCONNELL. Madam President, I have a substitute amendment at the desk that I ask the clerk to report.

The PRESIDING OFFICER. The clerk will report.

The legislative clerk read as follows:

The Senator from Kentucky [Mr. MCCONNELL] proposes an amendment numbered 1449.

Mr. MCCONNELL. I ask unanimous consent that the reading of the amendment be dispensed with.

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

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

Mr. MCCONNELL. I ask for the yeas and nays on my amendment.

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The yeas and nays were ordered.

AMENDMENT NO. 1450 TO AMENDMENT NO. 1449

Mr. MCCONNELL. Madam President, I have an amendment at the desk.

The PRESIDING OFFICER. The clerk will report.

The legislative clerk read as follows:

The Senator from Kentucky [Mr. MCCONNELL] proposes an amendment numbered 1450 to amendment No. 1449.

Mr. MCCONNELL. Madam President, I ask unanimous consent that the reading of the amendment be dispensed with.

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

The amendment is as follows:

Strike Sec. 110(a) and insert the following:

(a) IN GENERAL.—The amendments made by sections 101 through 103 shall take effect on the date that is 12 months after the date of the enactment of this Act.

Mr. MCCONNELL. I ask for the yeas and nays on my amendment.

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The yeas and nays were ordered.

AMENDMENT NO. 1451 TO AMENDMENT NO. 1450

Mr. MCCONNELL. I have a second-degree amendment at the desk.

The PRESIDING OFFICER. The clerk will report.

The legislative clerk read as follows:

The Senator from Kentucky [Mr. MCCONNELL] proposes an amendment numbered 1451 to amendment No. 1450.

The amendment is as follows:

(Purpose: To improve the amendment)

At the end, add the following:

(b) NONEFFECT OF CERTAIN PROVISIONS.—Section 401 of this Act, relating to appointment of amicus curiae, shall have no force or effect.

SEC. 110A. APPOINTMENT OF AMICUS CURIAE.

Section 103 (50 U.S.C. 1803) is amended by adding at the end the following new subsections:

''(i) AMICUS CURIAE.—

''(1) AUTHORIZATION.—A court established under subsection (a) or (b) is authorized, consistent with the requirement of subsection (c) and any other statutory requirement that the court act expeditiously or within a stated time—

''(A) to appoint amicus curiae to—

''(i) assist the court in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law; or

''(ii) provide technical expertise in any instance the court considers appropriate; or

''(B) upon motion, to permit an individual or organization leave to file an amicus curiae brief.

''(2) DESIGNATION.—The courts established by subsection (a) and (b) shall each designate 1 or more individuals who may be appointed to serve as amicus curiae and who are determined to be eligible for access to classified national security information necessary to participate in matters before such courts (if such access is necessary for participation in the matters for which they may be appointed). In appointing an amicus curiae pursuant to paragraph (1), the court may choose from among those so designated.

''(3) EXPERTISE.—An individual appointed as an amicus curiae under paragraph (1) may be an individual who possesses expertise on privacy and civil liberties, intelligence collection, communications technology, or any other area that may lend legal or technical expertise to the court.

''(4) DUTIES.—An amicus curiae appointed under paragraph (1) to assist with the consideration of a covered matter shall carry out the duties assigned by the appointing court. That court may authorize the amicus curiae to review any application, certification, petition, motion, or other submission that the court determines is relevant to the duties assigned by the court.

''(5) NOTIFICATION.—A court established under subsection (a) or (b) shall notify the Attorney General of each exercise of the authority to appoint an amicus curiae under paragraph (1).

''(6) ASSISTANCE.—A court established under subsection (a) or (b) may request and receive (including on a non-reimbursable basis) the assistance of the executive branch in the implementation of this subsection.

''(7) ADMINISTRATION.—A court established under subsection (a) or (b) may provide for the designation, appointment, removal, training, or other support of an amicus curiae appointed under paragraph (1) in a manner that is not inconsistent with this subsection.

''(j) REVIEW OF FISA COURT DECISIONS.—Following issuance of an order under this Act, a court established under subsection (a) shall certify for review to the court established under subsection (b) any question of law that may affect resolution of the matter in controversy that the court determines warrants such review because of a need for uniformity or because consideration by the court established under subsection (b) would serve the interests of justice. Upon certification of a question of law under this subsection, the court established under subsection (b) may give binding instructions or require the entire record to be sent up for decision of the entire matter in controversy.

''(k) REVIEW OF FISA COURT OF REVIEW DECISIONS.—

''(1) CERTIFICATION.—For purposes of section 1254(2) of title 28, United States Code, the court of review established under subsection (b) shall be considered to be a court of appeals.

''(2) AMICUS CURIAE BRIEFING.—Upon certification of an application under paragraph (1), the Supreme Court of the United States may appoint an amicus curiae designated under subsection (i)(3), or any other person, to provide briefing or other assistance.''.

AMENDMENT NO. 1452

Mr. MCCONNELL. I have an amendment to the text proposed to be stricken.

The PRESIDING OFFICER. The clerk will report.

The legislative clerk read as follows:

The Senator from Kentucky [Mr. MCCONNELL] proposes an amendment numbered 1452 to the language proposed to be stricken by amendment No. 1449.

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

Mr. MCCONNELL. I ask for the yeas and nays on my amendment.

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The yeas and nays were ordered.

AMENDMENT NO. 1453 TO AMENDMENT NO. 1452

Mr. MCCONNELL. I have a second-degree amendment at the desk.

The PRESIDING OFFICER. The clerk will report.

The legislative clerk read as follows:

The Senator from Kentucky [Mr. MCCONNELL] proposes an amendment numbered 1453 to amendment No. 1452.

The amendment is as follows:

At the end of the amendment, add the following:

''This Act shall take effect 1 day after the date of enactment.''

CLOTURE MOTION

Mr. MCCONNELL. Madam President, I have a cloture motion at the desk.

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

The 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 H.R. 2048, an act to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes.

Mitch McConnell, John Cornyn, Ron Johnson, Dean Heller, Steve Daines, Cory Gardner, Johnny Isakson, Richard Burr, Tim Scott, James Lankford, Jeff Flake, Mike Lee, Lisa Murkowski, John Barrasso, Thom Tillis, Chuck Grassley, Richard C. Shelby.

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2016—MOTION TO PROCEED

Mr. MCCONNELL. I move to proceed to H.R. 1735.

The PRESIDING OFFICER. The clerk will report the motion.

The legislative clerk read as follows:

Motion to proceed to Calendar No. 99, H.R. 1735, a bill to authorize appropriations for fiscal year 2016 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

CLOTURE MOTION

Mr. MCCONNELL. I send a cloture motion to the desk.

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

The 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 H.R. 1735, an act to authorize appropriations for fiscal year 2016 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

Mitch McConnell, John McCain, Lindsey Graham, Kelly Ayotte, Jeff Sessions, Shelley Moore Capito, Joni Ernst, Deb Fischer, Thom Tillis, Roger F. Wicker, Tom Cotton, Dan Sullivan, Mike Rounds, James M. Inhofe, John Cornyn, Mike Lee, Cory Gardner.

MORNING BUSINESS

Mr. MCCONNELL. Madam President, I ask unanimous consent that the Senate proceed to 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.

REMEMBERING BEAU BIDEN

Mrs. BOXER. Madam President, my heart and the hearts of my entire family go out to Vice President JOE BIDEN and his family on the tragic loss of his son, Beau Biden.

As a mother of children about Beau's age I know that this is the age when our children are coming fully into their own and Beau Biden was already there.

He was a skilled attorney general, a promising candidate for Governor, and above all an extraordinarily loving family member.

The Vice President has suffered too many losses in his lifetime and each one has cut deep. I hope he knows that all of us who love him are praying that his faith and the deep love of his family will see him through this tragic loss.

I know the people of California join me in sending the deepest condolences to the Biden family.

ADDITIONAL STATEMENTS

TRIBUTE TO C. EDWARD BROWN

• Mr. GRASSLEY. Madam President, I wish to recognize C. Edward ''Ed'' Brown, FACHE, on his election to the American Medical Group Association's Policy Hall of Fame. Ed has a long track record in Iowa and Washington as a leading advocate in health care policy reform. He also served in numerous leadership roles at the American Medical Group Association, chairing its public policy committee for 4 years and serving as chairman of its board.

Mr. Brown has had a distinguished career in health care in Iowa, where he has served for the last 21 years as chief executive officer of the Iowa Clinic, a multispecialty group practice in Des Moines. The Iowa Clinic is the largest physician-owned multispecialty group in central Iowa, with nearly 200 physicians and health care providers practicing in 40 specialties. The clinic serves a population area of 1.1 million, averaging 400,000 patient visits each year.

Ed has a long list of achievements in delivering cutting edge, quality-focused health care to the benefit of Iowans, and his achievements include the Iowa Clinic's adoption of electronic medical records and information technology systems. He holds a bachelor's degree in nursing from the University of Evansville and a master's degree in health administration from Washington University in St. Louis. Also, he is a fellow of the American College of Healthcare Executives, with more than 30 years of experience in executive and senior levels of health care management.

As an advocate for multispecialty medical groups and AMGA, Ed has been a leader in promoting a model of care delivery and an organization that represents some of the Nation's highest quality and most prestigious health care delivery systems. It is wonderful to see someone with such a distinguished health care record in Iowa recognized at the national level as a dedicated leader who is committed to improving health care at such an important time for our Nation's health care delivery system.

Ed's voice has been an invaluable contribution to the health care debate in this country, and I congratulate him on this deserved recognition for his countless achievements in the public policy realm. •

MESSAGE FROM THE HOUSE RECEIVED DURING ADJOURMENT

ENROLLED BILLS SIGNED

Under the authority of the order of the Senate on January 6, 2015, the Secretary of the Senate, on May 26, 2015, during the adjournment of the Senate, received a message from the House of Representatives announcing that the Speaker pro tempore (Mr. HARRIS) has signed the following enrolled bills:

H.R. 1690. An act to designate the United States courthouse located at 700 Grant Street in Pittsburgh, Pennsylvania, as the ''Joseph F. Weis Jr. United States Courthouse''.

H.R. 2353. An act to provide an extension of Federal-aid highway, highway safety, motor carrier safety, transit, and other programs funded out of the Highway Trust Fund, and for other purposes.

The enrolled bills were subsequently signed by the acting President pro tempore (Mr. BLUNT).

INTRODUCTION OF BILLS AND JOINT RESOLUTIONS

By Mr. VITTER:

S. 1470. A bill to amend the Small Business Act to provide additional assistance to small business concerns for disaster recovery, and for other purposes; to the Committee on Small Business and Entrepreneurship.

SUBMISSION OF CONCURRENT AND SENATE RESOLUTIONS

By Mr. CARDIN (for himself, Ms. COLLINS, Ms. CANTWELL, and Ms. AYOTTE):

S. Res. 188. A resolution expressing appreciation of the goals of American Craft Beer Week and commending the small and independent craft brewers of the United States; considered and agreed to.

SUBMITTED RESOLUTIONS

SENATE RESOLUTION 188—EXPRESSING APPRECIATION OF THE GOALS OF AMERICAN CRAFT BEER WEEK AND COMMENDING THE SMALL AND INDEPENDENT CRAFT BREWERS OF THE UNITED STATES

Mr. CARDIN (for himself, Ms. COLLINS, Ms. CANTWELL, and Ms. AYOTTE) submitted the following resolution; which was considered and agreed to:

S. RES. 188

Whereas American Craft Beer Week is celebrated annually in breweries, brew pubs, restaurants, and beer stores by craft brewers, home brewers, and beer enthusiasts nationwide;

Whereas in 2015, American Craft Beer Week is celebrated from May 11 to May 17;

Whereas craft brewers are a vibrant affirmation and expression of the entrepreneurial

traditions of the United States, operating as community-based small businesses, providing employment for 115,000 full- and part-time workers, and generating annually more than $3,000,000,000 in wages and benefits;

Whereas the United States has craft brewers in every State and more than 3,500 craft breweries nationwide, each producing fewer than 6,000,000 barrels of beer annually;

Whereas in 2014, 615 new breweries opened in the United States, creating jobs and improving economic conditions in communities across the United States;

Whereas in 2014, craft breweries in the United States produced more than 22,000,000 barrels of beer, which is 3,300,000 more barrels than craft breweries produced in 2013;

Whereas the craft brewers of the United States now export more than 383,000 barrels of beer and are establishing new markets abroad, which creates more domestic jobs to meet the growing international demand for craft beer from the United States;

Whereas the craft brewers of the United States support United States agriculture by purchasing barley, malt, and hops that are grown, processed, and distributed in the United States;

Whereas the craft brewers of the United States produce more than 100 distinct styles of flavorful beers, including many sought-after new and unique styles ranging from smoked porters to pumpkin peach ales that—

(1) contribute to a favorable balance of trade by reducing United States dependence on imported beers;

(2) support United States exports; and

(3) promote United States tourism;

Whereas craft beers from the United States consistently win international quality and taste awards;

Whereas the craft brewers of the United States strive to educate the people of the United States who are of legal drinking age about the differences in beer flavor, aroma, color, alcohol content, body, and other complex variables, the gastronomic qualities of beer, beer history, and historical brewing traditions dating back to colonial times and earlier;

Whereas the craft brewers of the United States champion the message of responsible enjoyment to their customers and work within their communities and the industry to prevent alcohol abuse and underage drinking;

Whereas the craft brewers of the United States are frequently involved in local communities through philanthropy, volunteerism, and sponsorship opportunities, including parent-teacher associations, Junior Reserve Officers' Training Corps (JROTC), hospitals for children, chambers of commerce, humane societies, rescue squads, athletic teams, and disease research;

Whereas the craft brewers of the United States are fully vested in the future success, health, welfare, and vitality of their communities as local employers who provide a diverse array of quality local jobs that will not be outsourced, who contribute to the local tax base; and who keep money in the United States by reinvesting in their businesses; and

Whereas increased Federal, State, and local support of craft brewing is important to fostering the continued growth of an industry of the United States that creates jobs, greatly benefits local economies, and brings international accolades to small businesses in the United States: Now, therefore, be it

Resolved, That the United States Senate—

(1) appreciates the goals of American Craft Beer Week, established by the Brewers Association, which represents the small craft brewers of the United States;

(2) recognizes the significant contributions of the craft brewers of the United States to the economy and to the communities in which the craft brewers are located; and

(3) commends the craft brewers of the United States for providing jobs, supporting United States agriculture, improving the balance of trade, and educating the people of the United States and beer lovers around the world about the history and culture of beer while promoting the legal and responsible consumption of beer.

AMENDMENTS SUBMITTED AND PROPOSED

SA 1441. Mr. PAUL (for himself and Mr. WYDEN) submitted an amendment intended to be proposed by him to the bill H.R. 2048, to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes; which was ordered to lie on the table.

SA 1442. Mr. PAUL submitted an amendment intended to be proposed by him to the bill H.R. 2048, supra; which was ordered to lie on the table.

SA 1443. Mr. PAUL (for himself and Mr. WYDEN) submitted an amendment intended to be proposed by him to the bill H.R. 2048, supra; which was ordered to lie on the table.

SA 1444. Mr. PAUL (for himself and Mr. WYDEN) submitted an amendment intended to be proposed by him to the bill H.R. 2048, supra; which was ordered to lie on the table.

SA 1445. Mr. PAUL submitted an amendment intended to be proposed by him to the bill H.R. 2048, supra; which was ordered to lie on the table.

SA 1446. Mr. PAUL submitted an amendment intended to be proposed by him to the bill H.R. 2048, supra; which was ordered to lie on the table.

SA 1447. Mr. PAUL (for himself and Mr. WYDEN) submitted an amendment intended to be proposed by him to the bill H.R. 2048, supra; which was ordered to lie on the table.

SA 1448. Mr. PAUL (for himself and Mr. WYDEN) submitted an amendment intended to be proposed by him to the bill H.R. 2048, supra; which was ordered to lie on the table.

SA 1449. Mr. MCCONNELL (for himself and Mr. BURR) proposed an amendment to the bill H.R. 2048, supra.

SA 1450. Mr. MCCONNELL proposed an amendment to amendment SA 1449 proposed by Mr. MCCONNELL (for himself and Mr. BURR) to the bill H.R. 2048, supra.

SA 1451. Mr. MCCONNELL proposed an amendment to amendment SA 1450 proposed by Mr. MCCONNELL to the amendment SA 1449 proposed by Mr. MCCONNELL (for himself and Mr. BURR) to the bill H .R. 2048, supra.

SA 1452. Mr. MCCONNELL (for himself and Mr. BURR) proposed an amendment to the bill H.R. 2048, supra.

SA 1453. Mr. MCCONNELL proposed an amendment to amendment SA 1452 proposed by Mr. MCCONNELL (for himself and Mr. BURR) to the bill H.R. 2048, supra.

TEXT OF AMENDMENTS ON MAY 22, 2015

SA 1440. Mr. SANDERS submitted an amendment intended to be proposed by him to the bill H.R. 2048, to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE IX—COMMISSION ON PRIVACY RIGHTS IN THE DIGITAL AGE

SECTION 901. SHORT TITLE.

This title may be cited as the ''Commission on Privacy Rights in the Digital Age Act of 2015''.

SEC. 902. FINDINGS.

Congress makes the following findings:

(1) Today, technology that did not exist 30 years ago pervades every aspect of life in the United States.

(2) Nearly ⅔ of adults in the United States own a smartphone, and 43 percent of adults in the United States rely solely on their cell phone for telephone use.

(3) 84 percent of households in the United States own a computer and 73 percent of households in the United States have a computer with an Internet broadband connection.

(4) Federal policies on privacy protection have not kept pace with the rapid expansion of technology.

(5) Innovations in technology have led to the exponential expansion of data collection by both the public and private sectors.

(6) Consumers are often unaware of the collection of their data and how their information can be collected, bought, and sold by private companies.

SEC. 903. PURPOSE.

The purpose of this title is to establish, for a 2-year period, a Commission on Privacy Rights in the Digital Age to—

(1) examine—

(A) the ways in which public agencies and private companies gather data on the people of the United States; and

(B) the ways in which that data is utilized, either internally or externally; and

(2) make recommendations concerning potential policy changes needed to safeguard the privacy of the people of the United States.

SEC. 904. COMPOSITION OF THE COMMISSION.

(a) ESTABLISHMENT.—To carry out the purpose of this title, there is established in the legislative branch a Commission on Privacy Rights in the Digital Age (in this title referred to as the ''Commission'').

(b) COMPOSITION.—The Commission shall be composed of 12 members, as follows:

(1) Four members appointed by the President, of whom—

(A) 2 shall be appointed from the executive branch of the Government; and

(B) 2 shall be appointed from private life.

(2) Two members appointed by the majority leader of the Senate, of whom—

(A) 1 shall be a Member of the Senate; and

(B) 1 shall be appointed from private life.

(3) Two members appointed by the minority leader of the Senate, of whom—

(A) 1 shall be a Member of the Senate; and

(B) 1 shall be appointed from private life.

(4) Two members appointed by the Speaker of the House of Representatives, of whom—

(A) 1 shall be a Member of the House; and

(B) 1 shall be appointed from private life.

(5) Two members appointed by the minority leader of the House of Representatives, of whom—

(A) 1 shall be a Member of the House; and

(B) 1 shall be appointed from private life.

(c) CHAIRPERSON.—The Commission shall elect a Chairperson and Vice-Chairperson from among its members.

(d) MEETINGS; QUORUM; VACANCIES.—

(1) MEETINGS.—After its initial meeting, the Commission shall meet upon the call of the Chairperson or a majority of its members.

(2) QUORUM.—Seven members of the Commission shall constitute a quorum.

(3) VACANCIES.—Any vacancy in the Commission shall not affect its powers but shall be filled in the same manner in which the original appointment was made.

(e) APPOINTMENT OF MEMBERS; INITIAL MEETING.—

(1) APPOINTMENT OF MEMBERS.—Each member of the Commission shall be appointed not later than 60 days after the date of enactment of this Act.

(2) INITIAL MEETING.—On or after the date on which all members of the Commission have been appointed, and not later than 60 days after the date of enactment of this Act, the Commission shall hold its initial meeting.

SEC. 905. DUTIES OF THE COMMISSION.

The Commission shall—

(1) conduct an investigation of relevant facts and circumstances relating to the expansion of data collection practices in the public, private, and national security sectors, including implications for—

(A) surveillance;

(B) political, civil, and commercial rights of individuals and corporate entities;

(C) employment practices, including hiring and firing; and

(D) credit availability and reporting; and

(2) submit to the President and Congress reports containing findings, conclusions, and recommendations for corrective measures relating to the facts and circumstances investigated under paragraph (1), in accordance with section 911.

SEC. 906. POWERS OF THE COMMISSION.

(a) IN GENERAL.—

(1) HEARINGS AND EVIDENCE.—The Commission or, at its direction, any subcommittee or member of the Commission, may, for the purpose of carrying out this title—

(A) hold such hearings, sit and act at such times and places, take such testimony, receive such evidence, and administer such oaths as the Commission or such subcommittee or member determines advisable; and

(B) subject to paragraph (2)(A), require, by subpoena or otherwise, the attendance and testimony of such witnesses and the production of such books, records, correspondence, memoranda, papers, documents, tapes, and materials as the Commission or such subcommittee or member determines advisable.

(2) SUBPOENAS.—

(A) ISSUANCE.—

(i) IN GENERAL.—A subpoena may be issued under paragraph (1) only—

(I) by the agreement of the Chairperson and the Vice Chairperson; or

(II) by the affirmative vote of 8 members of the Commission.

(ii) SIGNATURE.—Subject to clause (i), a subpoena issued under paragraph (1) may—

(I) be issued under the signature of—

(aa) the Chairperson; or

(bb) a member designated by a majority of the Commission; and

(II) be served by—

(aa) any person designated by the Chairperson; or

(bb) a member designated by a majority of the Commission.

(B) ENFORCEMENT.—

(i) IN GENERAL.—In the case of contumacy or failure to obey a subpoena issued under paragraph (1), the United States district court for the judicial district in which the subpoenaed person resides, is served, or may be found, or where the subpoena is returnable, may issue an order requiring such person to appear at any designated place to testify or to produce documentary or other evidence.

(ii) CONTEMPT OF COURT.—Any failure to obey the order of the court under clause (i) may be punished by the court as a contempt of that court.

(3) WITNESS ALLOWANCES AND FEES.—

(A) IN GENERAL.—Section 1821 of title 28, United States Code, shall apply to witnesses requested or subpoenaed to appear at any hearing of the Commission.

(B) SOURCE OF FUNDS.—The per diem and mileage allowances for witnesses shall be paid from funds available to pay the expenses of the Commission.

(b) CONTRACTING.—The Commission may, to such extent and in such amounts as are provided in appropriations Acts, enter into contracts to enable the Commission to discharge its duties under this title.

(c) INFORMATION FROM FEDERAL AGENCIES.—

(1) IN GENERAL.—The Commission may secure directly from any Federal department or agency such information as the Commission considers necessary to carry out this Act.

(2) FURNISHING OF INFORMATION.—If the Chairperson, the chairperson of any subcommittee created by a majority of the Commission, or any member designated by a majority of the Commission submits to a Federal department or agency a request for information under paragraph (1), the head of the department or agency shall, to the extent authorized by law, furnish the information directly to the Commission.

(3) RECEIPT, HANDLING, STORAGE, AND DISSEMINATION.—Information furnished under paragraph (2) shall only be received, handled, stored, and disseminated by members of the Commission and its staff consistent with all applicable statutes, regulations, and executive orders.

(d) ASSISTANCE FROM FEDERAL AGENCIES.—

(1) GENERAL SERVICES ADMINISTRATION.—The Administrator of General Services shall provide to the Commission on a reimbursable basis administrative support and other services for the performance of the Commission's functions.

(2) OTHER DEPARTMENTS AND AGENCIES.—In addition to the assistance provided under paragraph (1), departments and agencies of the United States may provide to the Commission such services, funds, facilities, staff, and other support services as the departments and agencies may determine advisable and as authorized by law.

(e) POSTAL SERVICES.—The Commission may use the United States mails in the same manner and under the same conditions as a department or agency of the United States.

SEC. 907. NONAPPLICABILITY OF FEDERAL ADVISORY COMMITTEE ACT.

(a) IN GENERAL.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Commission.

(b) PUBLIC MEETINGS AND RELEASE OF PUBLIC VERSIONS OF REPORTS.—The Commission shall—

(1) hold public hearings and meetings to the extent appropriate; and

(2) release public versions of the reports required under subsections (a) and (b) of section 911.

(c) PUBLIC HEARINGS.—Any public hearing of the Commission shall be conducted in a manner consistent with the protection of information provided to or developed for or by the Commission as required by any applicable statute, regulation, or executive order.

SEC. 908. STAFF OF COMMISSION.

(a) IN GENERAL.—

(1) APPOINTMENT AND COMPENSATION.—The Chairperson, in consultation with the Vice Chairperson and in accordance with rules agreed upon by the Commission, may appoint and fix the compensation of an executive director and such other personnel as may be necessary to enable the Commission to carry out the functions of the Commission, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to the provisions of chapter 51 and subchapter III of chapter 53 of that title relating to classification and General Schedule pay rates, except that no rate of pay fixed under this paragraph may exceed the equivalent of that payable for a position at level V of the Executive Schedule under section 5316 of title 5, United States Code.

(2) PERSONNEL AS FEDERAL EMPLOYEES.—

(A) IN GENERAL.—The executive director and any personnel of the Commission who are employees shall be employees under section 2105 of title 5, United States Code, for purposes of chapters 63, 81, 83, 84, 85, 87, 89, 89A, 89B, and 90 of that title.

(B) MEMBERS OF COMMISSION.—Subparagraph (A) shall not be construed to apply to members of the Commission.

(b) DETAILEES.—Any Federal Government employee may be detailed to the Commission without reimbursement from the Commission, and such detailee shall retain the rights, status, and privileges of his or her regular employment without interruption.

(c) CONSULTANT SERVICES.—The Commission may procure the services of experts and consultants in accordance with section 3109 of title 5, United States Code, but at rates not to exceed the daily rate paid a person occupying a position at level IV of the Executive Schedule under section 5315 of that title.

SEC. 909. COMPENSATION AND TRAVEL EXPENSES.

(a) COMPENSATION.—Each member of the Commission who is not an officer or employee of the Federal Government may be compensated at not to exceed the daily equivalent of the annual rate of basic pay in effect for a position at level IV of the Executive Schedule under section 5315 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Commission.

(b) TRAVEL EXPENSES.—While away from their homes or regular places of business in the performance of services for the Commission, members of the Commission shall be allowed travel expenses, including per diem in lieu of subsistence, in the same manner as persons employed intermittently in the Government service are allowed expenses under section 5703 of title 5, United States Code.

SEC. 910. SECURITY CLEARANCES FOR COMMISSION MEMBERS AND STAFF.

The appropriate departments or agencies of the Federal Government shall cooperate with the Commission in expeditiously providing to the members and staff of the Commission appropriate security clearances to the extent possible under applicable procedures and requirements, and no person shall be provided with access to classified information under this title without the appropriate security clearances.

SEC. 911. REPORTS OF COMMISSION; TERMINATION.

(a) INTERIM REPORTS.—The Commission shall submit to the President and Congress interim reports containing such findings, conclusions, and recommendations for corrective measures as have been agreed to by a majority of Commission members.

(b) FINAL REPORT.—Not later than 2 years after the date of enactment of this Act, the Commission shall submit to the President and Congress a final report containing such findings, conclusions, and recommendations

for corrective measures as have been agreed to by a majority of Commission members.

(c) CLASSIFIED INFORMATION.—Each report submitted under subsection (a) or (b) shall be in unclassified form, but may include a classified annex.

(d) TERMINATION.—

(1) IN GENERAL.—The Commission, and all the authorities under this title, shall terminate 60 days after the date on which Commission submits the final report under subsection (b).

(2) ADMINISTRATIVE ACTIVITIES BEFORE TERMINATION.—The Commission may use the 60-day period referred to in paragraph (1) for the purpose of concluding its activities, including providing testimony to committees of Congress concerning its reports and disseminating the final report.

SEC. 912. FUNDING.

(a) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as are necessary to carry out this title.

(b) DURATION OF AVAILABILITY.—Amounts made available to the Commission under subsection (a) shall remain available until the termination of the Commission.

TEXT OF AMENDMENTS

SA 1441. Mr. PAUL (for himself and Mr. WYDEN) submitted an amendment intended to be proposed by him to the bill H.R. 2048, to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes; which was ordered to lie on the table; as follows:

On page 4, strike line 20 and all that follows through page 5, line 4, and insert the following:

protect against international terrorism, a statement of facts showing that there is probable cause to believe that—

''(i) the call detail records sought to be produced based on the specific selection term required under subparagraph (A) are relevant to such investigation; and

''(ii) such specific selection term

SA 1442. Mr. PAUL submitted an amendment intended to be proposed by him to the bill H.R. 2048, to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes; which was ordered to lie on the table; as follows:

On page 29, line 6, strike the quotation marks and the second period and insert the following:

''(iii) LIMITATION TO ACTS OF TERRORISM AND ESPIONAGE.—Notwithstanding clauses (i) and (ii), no information obtained or evidence derived from a part of certification or procedure relating to which the Court orders a correction of a deficiency under subparagraph (B) shall be disclosed in a criminal case by the Government unless the defendant is charged with an act of espionage under chapter 37 of title 18, United States Code, or an act of terrorism (as defined under section 3077 of title 18, United States Code).''.

SA 1443. Mr. PAUL (for himself and Mr. WYDEN) submitted an amendment intended to be proposed by him to the bill H.R. 2048, to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. REQUIREMENT OF NOTICE TO DEFENDANTS.

(a) IN GENERAL.—

(1) ELECTRONIC SURVEILLANCE.—Section 106 (50 U.S.C. 1806) is amended by striking subsections (c) and (d) and inserting the following:

''(c)(1) Whenever the Government initiates a proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States against a person, the Government shall notify the person and the court or authority of—

''(A) each title of this Act the Government relied on to obtain the communications of the person or information about the communications or activities of the person, which contributed in any manner to the investigation of the person; and

''(B) each type of communication or information obtained under this Act, as described in the order or directive relied upon to obtain the communication or information.

''(2) The Government shall provide the notification required under paragraph (1) before or within a reasonable time after the commencement of the proceeding.

''(d) The notification requirement under subsection (c) shall apply to any State or political subdivision thereof whenever the State or political subdivision initiates a proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the State or political subdivision against a person, in the same manner such subsection applies to the Government in connection with a proceeding against a person.''.

(2) PHYSICAL SEARCHES.—Section 305 (50 U.S.C. 1825) is amended by striking subsections (d) and (e) and inserting the following:

''(d)(1) Whenever the Government initiates a proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States against a person, the Government shall notify the person and the court or authority of—

''(A) each title of this Act the Government relied on to obtain the communications of the person or information about the communications or activities of the person, which contributed in any manner to the investigation of the person; and

''(B) each type of communication or information obtained under this Act, as described in the order or directive relied upon to obtain the communication or information.

''(2) The Government shall provide the notification required under paragraph (1) before or within a reasonable time after the commencement of the proceeding.

''(e) The notification requirement under subsection (d) shall apply to any State or political subdivision thereof whenever the State or political subdivision initiates a proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the State or political subdivision against a person, in the same manner such subsection applies to the Government in connection with a proceeding against a person.''.

(3) PEN REGISTER AND TRAP AND TRACE DEVICES.—Section 405 (50 U.S.C. 1845) is amended by striking subsections (c) and (d) and inserting the following:

''(c)(1) Whenever the Government initiates a proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States against a person, the Government shall notify the person and the court or authority of—

''(A) each title of this Act the Government relied on to obtain the communications of the person or information about the communications or activities of the person, which contributed in any manner to the investigation of the person; and

''(B) each type of communication or information obtained under this Act, as described in the order or directive relied upon to obtain the communication or information.

''(2) The Government shall provide the notification required under paragraph (1) before or within a reasonable time after the commencement of the proceeding.

''(d) The notification requirement under subsection (c) shall apply to any State or political subdivision thereof whenever the State or political subdivision initiates a proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the State or political subdivision against a person, in the same manner such subsection applies to the Government in connection with a proceeding against a person.''.

(b) TANGIBLE THINGS.—Section 501 (50 U.S.C. 1861), as amended by section 107 of this Act, is amended by adding at the end the following:

''(l) SUPPRESSION OF EVIDENCE.—

''(1) MOTION TO SUPPRESS.—

''(A) IN GENERAL.—Any person against whom evidence obtained or derived from the production of tangible things under this title is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from the production of the communications of the person or information about the communications or activities of the person on the grounds that—

''(i) the information was unlawfully acquired; or

''(ii) the production was not made in accordance with an order of authorization or approval.

''(B) TIMING.—A motion described in subparagraph (A) shall be made before the trial, hearing, or other proceeding commences, unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

''(2) IN CAMERA AND EX PARTE REVIEW BY COURT.—

''(A) DEFINITION.—In this paragraph, the term 'covered circumstance' means—

''(i) that—

''(I) a court or authority receives a notice under subsection (c) or (d) of section 106, subsection (d) or (e) of section 305, or subsection (c) or (d) of section 405 that relates to the production of tangible things under this title;

''(II) a motion is made under paragraph (1) of this subsection; or

''(III) a motion or request is made by a person under any other statute or rule of the United States or any State before a court or authority of the United States or any State to—

''(aa) discover or obtain applications or orders or other materials relating to the production of tangible things under this title; or

''(bb) discover, obtain, or suppress evidence or information obtained or derived from the

production of tangible things under this title; and

''(ii) that the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States.

''(B) AUTHORITY.—In a covered circumstance, the applicable district court of the United States, or if notice is given to or the motion is made before another authority, the district court of the United States in the same judicial district as the authority, shall review in camera and ex parte the application, order, and such other materials relating to the production of tangible things under this title as may be necessary to determine whether the production was lawfully authorized and conducted.

''(C) DISCLOSURE.—In making a determination under subparagraph (B), the court may disclose to the applicable person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the production only if such disclosure would aid the court in making an accurate determination of the legality of the surveillance.

''(3) SUPPRESSION OF EVIDENCE; DENIAL OF MOTION.—If a district court of the United States determines under paragraph (2) that the production of tangible things under this title was not lawfully authorized or conducted, the court shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from the production or otherwise grant the motion of the movant. If the court determines that the production was lawfully authorized and conducted, it shall deny the motion of the movant except to the extent that due process requires discovery or disclosure.

''(4) FINALITY OF ORDERS.—An order granting a motion or request under paragraph (3), a determination under this subsection that the production of tangible things under this title was not lawfully authorized or conducted, and an order of a district court of the United States requiring review or granting disclosure of an application, order, or other material relating to the production of tangible things under this title shall be a final order and binding upon all courts of the United States and the several States, except a United States court of appeals and the Supreme Court of the United States.

''(5) DESTRUCTION OF UNLAWFULLY OBTAINED EVIDENCE.—If a district court of the United States determines under paragraph (2) that the production of tangible things under this title was not lawfully authorized or conducted, the determination is a final order under paragraph (4), and the district court finds there is no reason to believe that destruction may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person, the Government shall destroy all copies of the tangible things produced under this title in the possession of the Government by not later than 30 days after the date of issuance of the final court order.''.

SA 1444. Mr. PAUL (for himself and Mr. WYDEN) submitted an amendment intended to be proposed by him to the bill H.R. 2048, to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes; which was ordered to lie on the table; as follows:

On page 17, line 4, strike ''an electronic'' and all that follows through ''Code)'' on line 9 and insert ''a corporation or other legal entity''.

SA 1445. Mr. PAUL submitted an amendment intended to be proposed by him to the bill H.R. 2048, to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. COURT APPROVAL FOR NATIONAL SECURITY LETTERS.

(a) IN GENERAL.—Section 2709(b) of title 18, United States Code, is amended—

(1) in the subsection heading, by striking ''REQUIRED CERTIFICATION'' and inserting ''REQUEST UPON AUTHORIZATION BY COURT''; and

(2) in the matter preceding paragraph (1), by striking ''The Director'' and inserting ''If authorized by an order of a Federal court (other than the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a))), the Director''.

(b) RIGHT TO FINANCIAL PRIVACY ACT OF 1978.—Section 1114(a)(5)(A) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(5)(A)) is amended by adding at the end the following: ''A certification may only be made under this subparagraph if authorized by an order of a Federal court (other than the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a))).''.

(c) FAIR CREDIT REPORTING ACT.—The Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) is amended—

(1) in section 626 (15 U.S.C. 1681u)—

(A) in subsection (a), in the second sentence, by inserting ''if authorized by an order of a Federal court (other than the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a))) and'' after ''The Director or the Director's designee may make such a certification only''; and

(B) in subsection (b), in the second sentence, by inserting ''if authorized by an order of a Federal court (other than the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a))) and'' after ''The Director or the Director's designee may make such a certification only''; and

(2) in section 627(b) (15 U.S.C. 1681v(b))—

(A) in the subsection heading, by striking ''FORM OF'' and inserting ''REQUIREMENTS FOR''; and

(B) by striking ''described in subsection (a) shall be signed'' and inserting the following: ''described in subsection (a)—

''(1) may only be made if authorized by an order of a Federal court (other than the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a))); and

''(2) shall be signed''.

SA 1446. Mr. PAUL submitted an amendment intended to be proposed by him to the bill H.R. 2048, to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. FOURTH AMENDMENT PRESERVATION AND PROTECTION.

(a) SHORT TITLE.—This section may be cited as the ''Fourth Amendment Preservation and Protection Act of 2015''.

(b) FINDINGS.—Congress finds that the right under the Fourth Amendment to the Constitution of the United States of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures is violated when the Federal Government or a State or local government acquires information voluntarily relinquished by a person to another party for a limited business purpose without the express informed consent of the person to the specific request by the Federal Government or a State or local government or a warrant, upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

(c) DEFINITION.—In this section, the term ''system of records'' means any group of records from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular associated with the individual.

(d) PROHIBITION.—

(1) IN GENERAL.—Except as provided in paragraph (2), the Federal Government and a State or local government may not obtain or seek to obtain information relating to an individual or group of individuals held by a third party in a system of records, and no such information shall be admissible in a criminal prosecution in a court of law.

(2) EXCEPTION.—The Federal Government or a State or local government may obtain, and a court may admit, information relating to an individual held by a third party in a system of records if—

(A) the individual whose name or identification information the Federal Government or State or local government is using to access the information provides express and informed consent to the search; or

(B) the Federal Government or State or local government obtains a warrant, upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

SA 1447. Mr. PAUL (for himself and Mr. WYDEN) submitted an amendment intended to be proposed by him to the bill H.R. 2048, to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. CLARIFICATION ON PROHIBITION ON SEARCHING OF COLLECTIONS OF COMMUNICATIONS TO CONDUCT WARRANTLESS SEARCHES FOR THE COMMUNICATIONS OF UNITED STATES PERSONS.

Section 702(b) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(b)) is amended—

(1) by redesignating paragraphs (1) through (5) as subparagraphs (A) through (E), respectively, and indenting such subparagraphs, as so redesignated, an additional two ems from the left margin;

(2) by striking ''An acquisition'' and inserting the following:

''(1) IN GENERAL.—An acquisition''; and

(3) by adding at the end the following:

''(2) CLARIFICATION ON PROHIBITION ON SEARCHING OF COLLECTIONS OF COMMUNICATIONS OF UNITED STATES PERSONS.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), no officer or employee of the United States may conduct a search of a collection of communications acquired under this section in an effort to find communications of a particular United States person (other than a corporation).

''(B) CONCURRENT AUTHORIZATION AND EXCEPTION FOR EMERGENCY SITUATIONS.—Subparagraph (A) shall not apply to a search for communications related to a particular United States person if—

''(i) such United States person is the subject of an order or emergency authorization authorizing electronic surveillance or physical search under section 105, 304, 703, 704, or 705 of this Act, or under title 18, United States Code, for the effective period of that order;

''(ii) the entity carrying out the search has a reasonable belief that the life or safety of such United States person is threatened and the information is sought for the purpose of assisting that person; or

''(iii) such United States person has consented to the search.''.

SA 1448. Mr. PAUL (for himself and Mr. WYDEN) submitted an amendment intended to be proposed by him to the bill H.R. 2048, to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ____. PROHIBITION ON DATA SECURITY VULNERABILITY MANDATES.

(a) IN GENERAL.—Except as provided in subsection (b), no agency may mandate that a manufacturer, developer, or seller of covered products design or alter the security functions in its product or service to allow the surveillance of any user of such product or service, or to allow the physical search of such product, by any agency.

(b) EXCEPTION.—Subsection (a) shall not apply to mandates authorized under the Communications Assistance for Law Enforcement Act (47 U.S.C. 1001 et seq.).

(c) DEFINITIONS.—In this section—

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

(2) the term ''covered product'' means any computer hardware, computer software, or electronic device that is made available to the general public.

SA 1449. Mr. MCCONNELL (for himself and Mr. BURR) proposed an amendment to the bill H.R. 2048, to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes; as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015'' or the ''USA FREEDOM Act of 2015''.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

1. Short title; table of contents.
2. Amendments to the Foreign Intelligence Surveillance Act of 1978.

TITLE I—FISA BUSINESS RECORDS REFORMS

101. Additional requirements for call detail records.
102. Emergency authority.
103. Prohibition on bulk collection of tangible things.
104. Judicial review.
105. Liability protection.
106. Compensation for assistance.
107. Notice to the Attorney General on changes in retention of call detail records.
108. Definitions.
109. Inspector General reports on business records orders.
110. Effective date.
111. Rule of construction.

TITLE II—FISA PEN REGISTER AND TRAP AND TRACE DEVICE REFORM

201. Prohibition on bulk collection.
202. Privacy procedures.

TITLE III—FISA ACQUISITIONS TARGETING PERSONS OUTSIDE THE UNITED STATES REFORMS

301. Limits on use of unlawfully obtained information.

TITLE IV—FOREIGN INTELLIGENCE SURVEILLANCE COURT REFORMS

401. Appointment of amicus curiae.
402. Declassification of decisions, orders, and opinions.

TITLE V—NATIONAL SECURITY LETTER REFORM

501. Prohibition on bulk collection.
502. Limitations on disclosure of national security letters.
503. Judicial review.

TITLE VI—FISA TRANSPARENCY AND REPORTING REQUIREMENTS

601. Additional reporting on orders requiring production of business records; business records compliance reports to Congress.
602. Annual reports by the Government.
603. Public reporting by persons subject to FISA orders.
604. Reporting requirements for decisions, orders, and opinions of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review.
605. Submission of reports under FISA.

TITLE VII—ENHANCED NATIONAL SECURITY PROVISIONS

701. Emergencies involving non-United States persons.
702. Preservation of treatment of non-United States persons traveling outside the United States as agents of foreign powers.
703. Improvement to investigations of international proliferation of weapons of mass destruction.
704. Increase in penalties for material support of foreign terrorist organizations.
705. Sunsets.

TITLE VIII—SAFETY OF MARITIME NAVIGATION AND NUCLEAR TERRORISM CONVENTIONS IMPLEMENTATION

Subtitle A—Safety of Maritime Navigation

801. Amendment to section 2280 of title 18, United States Code.
802. New section 2280a of title 18, United States Code.
803. Amendments to section 2281 of title 18, United States Code.
804. New section 2281a of title 18, United States Code.
805. Ancillary measure.

Subtitle B—Prevention of Nuclear Terrorism

811. New section 2332i of title 18, United States Code.
812. Amendment to section 831 of title 18, United States Code.

SEC. 2. AMENDMENTS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

Except as otherwise expressly provided, whenever in this Act an amendment or repeal is expressed in terms of an amendment to, or a repeal of, a section or other provision, the reference shall be considered to be made to a section or other provision of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

TITLE I—FISA BUSINESS RECORDS REFORMS

SEC. 101. ADDITIONAL REQUIREMENTS FOR CALL DETAIL RECORDS.

(a) APPLICATION.—Section 501(b)(2) (50 U.S.C. 1861(b)(2)) is amended—

(1) in subparagraph (A)—

(A) in the matter preceding clause (i), by striking ''a statement'' and inserting ''in the case of an application other than an application described in subparagraph (C) (including an application for the production of call detail records other than in the manner described in subparagraph (C)), a statement''; and

(B) in clause (iii), by striking ''; and'' and inserting a semicolon;

(2) by redesignating subparagraphs (A) and (B) as subparagraphs (B) and (D), respectively; and

(3) by inserting after subparagraph (B) (as so redesignated) the following new subparagraph:

''(C) in the case of an application for the production on an ongoing basis of call detail records created before, on, or after the date of the application relating to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to protect against international terrorism, a statement of facts showing that—

''(i) there are reasonable grounds to believe that the call detail records sought to be produced based on the specific selection term required under subparagraph (A) are relevant to such investigation; and

''(ii) there is a reasonable, articulable suspicion that such specific selection term is associated with a foreign power engaged in international terrorism or activities in preparation therefor, or an agent of a foreign power engaged in international terrorism or activities in preparation therefor; and''.

(b) ORDER.—Section 501(c)(2) (50 U.S.C. 1861(c)(2)) is amended—

(1) in subparagraph (D), by striking ''; and'' and inserting a semicolon;

(2) in subparagraph (E), by striking the period and inserting ''; and''; and

(3) by adding at the end the following new subparagraph:

''(F) in the case of an application described in subsection (b)(2)(C), shall—

''(i) authorize the production on a daily basis of call detail records for a period not to exceed 180 days;

''(ii) provide that an order for such production may be extended upon application under subsection (b) and the judicial finding under paragraph (1) of this subsection;

''(iii) provide that the Government may require the prompt production of a first set of call detail records using the specific selection term that satisfies the standard required under subsection (b)(2)(C)(ii);

''(iv) provide that the Government may require the prompt production of a second set of call detail records using session-identifying information or a telephone calling card number identified by the specific selection term used to produce call detail records under clause (iii);

''(v) provide that, when produced, such records be in a form that will be useful to the Government;

''(vi) direct each person the Government directs to produce call detail records under the order to furnish the Government forthwith all information, facilities, or technical assistance necessary to accomplish the production in such a manner as will protect the secrecy of the production and produce a minimum of interference with the services that such person is providing to each subject of the production; and

''(vii) direct the Government to—

''(I) adopt minimization procedures that require the prompt destruction of all call detail records produced under the order that the Government determines are not foreign intelligence information; and

''(II) destroy all call detail records produced under the order as prescribed by such procedures.''.

SEC. 102. EMERGENCY AUTHORITY.

(a) AUTHORITY.—Section 501 (50 U.S.C. 1861) is amended by adding at the end the following new subsection:

''(i) EMERGENCY AUTHORITY FOR PRODUCTION OF TANGIBLE THINGS.—

''(1) Notwithstanding any other provision of this section, the Attorney General may require the emergency production of tangible things if the Attorney General—

''(A) reasonably determines that an emergency situation requires the production of tangible things before an order authorizing such production can with due diligence be obtained;

''(B) reasonably determines that the factual basis for the issuance of an order under this section to approve such production of tangible things exists;

''(C) informs, either personally or through a designee, a judge having jurisdiction under this section at the time the Attorney General requires the emergency production of tangible things that the decision has been made to employ the authority under this subsection; and

''(D) makes an application in accordance with this section to a judge having jurisdiction under this section as soon as practicable, but not later than 7 days after the Attorney General requires the emergency production of tangible things under this subsection.

''(2) If the Attorney General requires the emergency production of tangible things under paragraph (1), the Attorney General shall require that the minimization procedures required by this section for the issuance of a judicial order be followed.

''(3) In the absence of a judicial order approving the production of tangible things under this subsection, the production shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time the Attorney General begins requiring the emergency production of such tangible things, whichever is earliest.

''(4) A denial of the application made under this subsection may be reviewed as provided in section 103.

''(5) If such application for approval is denied, or in any other case where the production of tangible things is terminated and no order is issued approving the production, no information obtained or evidence derived from such production shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof, and no information concerning any United States person acquired from such production shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

''(6) The Attorney General shall assess compliance with the requirements of paragraph (5).''.

(b) CONFORMING AMENDMENT.—Section 501(d) (50 U.S.C. 1861(d)) is amended—

(1) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking ''pursuant to an order'' and inserting ''pursuant to an order issued or an emergency production required'';

(B) in subparagraph (A), by striking ''such order'' and inserting ''such order or such emergency production''; and

(C) in subparagraph (B), by striking ''the order'' and inserting ''the order or the emergency production''; and

(2) in paragraph (2)—

(A) in subparagraph (A), by striking ''an order'' and inserting ''an order or emergency production''; and

(B) in subparagraph (B), by striking ''an order'' and inserting ''an order or emergency production''.

SEC. 103. PROHIBITION ON BULK COLLECTION OF TANGIBLE THINGS.

(a) APPLICATION.—Section 501(b)(2) (50 U.S.C. 1861(b)(2)), as amended by section 101(a) of this Act, is further amended by inserting before subparagraph (B), as redesignated by such section 101(a) of this Act, the following new subparagraph:

''(A) a specific selection term to be used as the basis for the production of the tangible things sought;''.

(b) ORDER.—Section 501(c) (50 U.S.C. 1861(c)) is amended—

(1) in paragraph (2)(A), by striking the semicolon and inserting '', including each specific selection term to be used as the basis for the production;''; and

(2) by adding at the end the following new paragraph:

''(3) No order issued under this subsection may authorize the collection of tangible things without the use of a specific selection term that meets the requirements of subsection (b)(2).''.

SEC. 104. JUDICIAL REVIEW.

(a) MINIMIZATION PROCEDURES.—

(1) JUDICIAL REVIEW.—Section 501(c)(1) (50 U.S.C. 1861(c)(1)) is amended by inserting after ''subsections (a) and (b)'' the following: ''and that the minimization procedures submitted in accordance with subsection (b)(2)(D) meet the definition of minimization procedures under subsection (g)''.

(2) RULE OF CONSTRUCTION.—Section 501(g) (50 U.S.C. 1861(g)) is amended by adding at the end the following new paragraph:

''(3) RULE OF CONSTRUCTION.—Nothing in this subsection shall limit the authority of the court established under section 103(a) to impose additional, particularized minimization procedures with regard to the production, retention, or dissemination of nonpublicly available information concerning unconsenting United States persons, including additional, particularized procedures related to the destruction of information within a reasonable time period.''.

(3) TECHNICAL AND CONFORMING AMENDMENT.—Section 501(g)(1) (50 U.S.C. 1861(g)(1)) is amended—

(A) by striking ''Not later than 180 days after the date of the enactment of the USA PATRIOT Improvement and Reauthorization Act of 2005, the'' and inserting ''The''; and

(B) by inserting after ''adopt'' the following: '', and update as appropriate,''.

(b) ORDERS.—Section 501(f)(2) (50 U.S.C. 1861(f)(2)) is amended—

(1) in subparagraph (A)(i)—

(A) by striking ''that order'' and inserting ''the production order or any nondisclosure order imposed in connection with the production order''; and

(B) by striking the second sentence; and

(2) in subparagraph (C)—

(A) by striking clause (ii); and

(B) by redesignating clause (iii) as clause (ii).

SEC. 105. LIABILITY PROTECTION.

Section 501(e) (50 U.S.C. 1861(e)) is amended to read as follows:

''(e)(1) No cause of action shall lie in any court against a person who—

''(A) produces tangible things or provides information, facilities, or technical assistance in accordance with an order issued or an emergency production required under this section; or

''(B) otherwise provides technical assistance to the Government under this section or to implement the amendments made to this section by the USA FREEDOM Act of 2015.

''(2) A production or provision of information, facilities, or technical assistance described in paragraph (1) shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.''.

SEC. 106. COMPENSATION FOR ASSISTANCE.

Section 501 (50 U.S.C. 1861), as amended by section 102 of this Act, is further amended by adding at the end the following new subsection:

''(j) COMPENSATION.—The Government shall compensate a person for reasonable expenses incurred for—

''(1) producing tangible things or providing information, facilities, or assistance in accordance with an order issued with respect to an application described in subsection (b)(2)(C) or an emergency production under subsection (i) that, to comply with subsection (i)(1)(D), requires an application described in subsection (b)(2)(C); or

''(2) otherwise providing technical assistance to the Government under this section or to implement the amendments made to this section by the USA FREEDOM Act of 2015.''.

SEC. 107. NOTICE TO THE ATTORNEY GENERAL ON CHANGES IN RETENTION OF CALL DETAIL RECORDS.

Section 501 (50 U.S.C. 1861), as amended by section 106 of this Act, is amended by adding at the end the following new subsection:

''(k) PROSPECTIVE CHANGES TO EXISTING PRACTICES RELATED TO CALL DETAIL RECORDS.—

''(1) IN GENERAL.—Consistent with subsection (c)(2)(F), an electronic communication service provider that has been issued an order to produce call detail records pursuant to an order under subsection (c) shall notify the Attorney General if that service provider intends to retain its call detail records for a period less than 18 months.

''(2) TIMING OF NOTICE.—A notification under paragraph (1) shall be made not less than 180 days prior to the date such electronic communications service provider intends to implement a policy to retain such records for a period less than 18 months.''.

SEC. 108. DEFINITIONS.

Section 501 (50 U.S.C. 1861), as amended by section 107 of this Act, is further amended by adding at the end the following new subsection:

''(l) DEFINITIONS.—In this section:

''(1) IN GENERAL.—The terms 'foreign power', 'agent of a foreign power', 'international terrorism', 'foreign intelligence information', 'Attorney General', 'United States person', 'United States', 'person', and 'State' have the meanings provided those terms in section 101.

''(2) ADDRESS.—The term 'address' means a physical address or electronic address, such as an electronic mail address or temporarily assigned network address (including an Internet protocol address).

''(3) CALL DETAIL RECORD.—The term 'call detail record'—

''(A) means session-identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity number, or an International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call; and

''(B) does not include—

''(i) the contents (as defined in section 2510(8) of title 18, United States Code) of any communication;

''(ii) the name, address, or financial information of a subscriber or customer; or

''(iii) cell site location or global positioning system information.

''(4) SPECIFIC SELECTION TERM.—

''(A) TANGIBLE THINGS.—

''(i) IN GENERAL.—Except as provided in subparagraph (B), a 'specific selection term'—

''(I) is a term that specifically identifies a person, account, address, or personal device, or any other specific identifier; and

''(II) is used to limit, to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things.

''(ii) LIMITATION.—A specific selection term under clause (i) does not include an identifier that does not limit, to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things, such as an identifier that—

''(I) identifies an electronic communication service provider (as that term is defined in section 701) or a provider of remote computing service (as that term is defined in section 2711 of title 18, United States Code), when not used as part of a specific identifier as described in clause (i), unless the provider is itself a subject of an authorized investigation for which the specific selection term is used as the basis for the production; or

''(II) identifies a broad geographic region, including the United States, a city, a county, a State, a zip code, or an area code, when not used as part of a specific identifier as described in clause (i).

''(iii) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to preclude the use of multiple terms or identifiers to meet the requirements of clause (i).

''(B) CALL DETAIL RECORD APPLICATIONS.—For purposes of an application submitted under subsection (b)(2)(C), the term 'specific selection term' means a term that specifically identifies an individual, account, or personal device.''.

SEC. 109. INSPECTOR GENERAL REPORTS ON BUSINESS RECORDS ORDERS.

Section 106A of the USA PATRIOT Improvement and Reauthorization Act of 2005 (Public Law 109–177; 120 Stat. 200) is amended—

(1) in subsection (b)—

(A) in paragraph (1), by inserting ''and calendar years 2012 through 2014'' after ''2006'';

(B) by striking paragraphs (2) and (3);

(C) by redesignating paragraphs (4) and (5) as paragraphs (2) and (3), respectively; and

(D) in paragraph (3) (as so redesignated)—

(i) by striking subparagraph (C) and inserting the following new subparagraph:

''(C) with respect to calendar years 2012 through 2014, an examination of the minimization procedures used in relation to orders under section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861) and whether the minimization procedures adequately protect the constitutional rights of United States persons;''; and

(ii) in subparagraph (D), by striking ''(as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)))'';

(2) in subsection (c), by adding at the end the following new paragraph:

''(3) CALENDAR YEARS 2012 THROUGH 2014.—Not later than 1 year after the date of enactment of the USA FREEDOM Act of 2015, the Inspector General of the Department of Justice shall submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives a report containing the results of the audit conducted under subsection (a) for calendar years 2012 through 2014.'';

(3) by redesignating subsections (d) and (e) as subsections (e) and (f), respectively;

(4) by inserting after subsection (c) the following new subsection:

''(d) INTELLIGENCE ASSESSMENT.—

''(1) IN GENERAL.—For the period beginning on January 1, 2012, and ending on December 31, 2014, the Inspector General of the Intelligence Community shall assess—

''(A) the importance of the information acquired under title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) to the activities of the intelligence community;

''(B) the manner in which that information was collected, retained, analyzed, and disseminated by the intelligence community;

''(C) the minimization procedures used by elements of the intelligence community under such title and whether the minimization procedures adequately protect the constitutional rights of United States persons; and

''(D) any minimization procedures proposed by an element of the intelligence community under such title that were modified or denied by the court established under section 103(a) of such Act (50 U.S.C. 1803(a)).

''(2) SUBMISSION DATE FOR ASSESSMENT.—Not later than 180 days after the date on which the Inspector General of the Department of Justice submits the report required under subsection (c)(3), the Inspector General of the Intelligence Community shall submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives a report containing the results of the assessment for calendar years 2012 through 2014.'';

(5) in subsection (e), as redesignated by paragraph (3)—

(A) in paragraph (1)—

(i) by striking ''a report under subsection (c)(1) or (c)(2)'' and inserting ''any report under subsection (c) or (d)''; and

(ii) by striking ''Inspector General of the Department of Justice'' and inserting ''Inspector General of the Department of Justice, the Inspector General of the Intelligence Community, and any Inspector General of an element of the intelligence community that prepares a report to assist the Inspector General of the Department of Justice or the Inspector General of the Intelligence Community in complying with the requirements of this section''; and

(B) in paragraph (2), by striking ''the reports submitted under subsections (c)(1) and (c)(2)'' and inserting ''any report submitted under subsection (c) or (d)'';

(6) in subsection (f), as redesignated by paragraph (3)—

(A) by striking ''The reports submitted under subsections (c)(1) and (c)(2)'' and inserting ''Each report submitted under subsection (c)''; and

(B) by striking ''subsection (d)(2)'' and inserting ''subsection (e)(2)''; and

(7) by adding at the end the following new subsection:

''(g) DEFINITIONS.—In this section:

''(1) INTELLIGENCE COMMUNITY.—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).

''(2) UNITED STATES PERSON.—The term 'United States person' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).''.

SEC. 110. EFFECTIVE DATE.

(a) IN GENERAL.—The amendments made by sections 101 through 103 shall take effect on the date that is 180 days after the date of the enactment of this Act.

(b) REVIEW AND CERTIFICATION.—The Director of National Intelligence shall—

(1) review the implementation of the transition from the existing procedures for the production of call detail records under title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as in effect prior to the effective date for the amendments made by sections 101 through 103 of this Act, to the new procedures pursuant to the amendments made by sections 101 through 103 of this Act; and

(2) not later than 30 days before the effective date specified in subsection (a), certify to Congress in writing that—

(A) the implementation of the transition described in paragraph (1) is operationally effective to allow the timely retrieval of foreign intelligence information from recipients of an order issued under section 501(c)(2)(F) of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101 of this Act; and

(B) the implementation of the amendments made by section 101 through 103 of this Act—

(i) will not harm the national security of the United States; and

(ii) will ensure the protection of classified information and classified intelligence sources and methods related to such production of call detail records.

(c) RULE OF CONSTRUCTION.—Nothing in this Act shall be construed to alter or eliminate the authority of the Government to obtain an order under title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) as in effect prior to the effective date described in subsection (a) during the period ending on such effective date.

SEC. 111. RULE OF CONSTRUCTION.

Nothing in this Act shall be construed to authorize the production of the contents (as such term is defined in section 2510(8) of title 18, United States Code) of any electronic communication from an electronic communication service provider (as such term is defined in section 701(b)(4) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881(b)(4))) under title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.).

TITLE II—FISA PEN REGISTER AND TRAP AND TRACE DEVICE REFORM

SEC. 201. PROHIBITION ON BULK COLLECTION.

(a) PROHIBITION.—Section 402(c) (50 U.S.C. 1842(c)) is amended—

(1) in paragraph (1), by striking ''; and'' and inserting a semicolon;

(2) in paragraph (2), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following new paragraph:

''(3) a specific selection term to be used as the basis for the use of the pen register or trap and trace device.''.

(b) DEFINITION.—Section 401 (50 U.S.C. 1841) is amended by adding at the end the following new paragraph:

''(4)(A) The term 'specific selection term'—

''(i) is a term that specifically identifies a person, account, address, or personal device, or any other specific identifier; and

''(ii) is used to limit, to the greatest extent reasonably practicable, the scope of information sought, consistent with the purpose for seeking the use of the pen register or trap and trace device.

''(B) A specific selection term under subparagraph (A) does not include an identifier that does not limit, to the greatest extent reasonably practicable, the scope of information sought, consistent with the purpose for seeking the use of the pen register or trap and trace device, such as an identifier that—

''(i) identifies an electronic communication service provider (as that term is defined in section 701) or a provider of remote computing service (as that term is defined in section 2711 of title 18, United States Code), when not used as part of a specific identifier as described in subparagraph (A), unless the provider is itself a subject of an authorized investigation for which the specific selection term is used as the basis for the use; or

''(ii) identifies a broad geographic region, including the United States, a city, a county, a State, a zip code, or an area code, when not used as part of a specific identifier as described in subparagraph (A).

''(C) For purposes of subparagraph (A), the term 'address' means a physical address or electronic address, such as an electronic mail address or temporarily assigned network address (including an Internet protocol address).

''(D) Nothing in this paragraph shall be construed to preclude the use of multiple terms or identifiers to meet the requirements of subparagraph (A).''.

SEC. 202. PRIVACY PROCEDURES.

(a) IN GENERAL.—Section 402 (50 U.S.C. 1842) is amended by adding at the end the following new subsection:

''(h) PRIVACY PROCEDURES.—

''(1) IN GENERAL.—The Attorney General shall ensure that appropriate policies and procedures are in place to safeguard nonpublicly available information concerning United States persons that is collected through the use of a pen register or trap and trace device installed under this section. Such policies and procedures shall, to the maximum extent practicable and consistent with the need to protect national security, include privacy protections that apply to the collection, retention, and use of information concerning United States persons.

''(2) RULE OF CONSTRUCTION.—Nothing in this subsection limits the authority of the court established under section 103(a) or of the Attorney General to impose additional privacy or minimization procedures with regard to the installation or use of a pen register or trap and trace device.''.

(b) EMERGENCY AUTHORITY.—Section 403 (50 U.S.C. 1843) is amended by adding at the end the following new subsection:

''(d) PRIVACY PROCEDURES.—Information collected through the use of a pen register or trap and trace device installed under this section shall be subject to the policies and procedures required under section 402(h).''.

TITLE III—FISA ACQUISITIONS TARGETING PERSONS OUTSIDE THE UNITED STATES REFORMS

SEC. 301. LIMITS ON USE OF UNLAWFULLY OBTAINED INFORMATION.

Section 702(i)(3) (50 U.S.C. 1881a(i)(3)) is amended by adding at the end the following new subparagraph:

''(D) LIMITATION ON USE OF INFORMATION.—

''(i) IN GENERAL.—Except as provided in clause (ii), if the Court orders a correction of a deficiency in a certification or procedures under subparagraph (B), no information obtained or evidence derived pursuant to the part of the certification or procedures that has been identified by the Court as deficient concerning any United States person shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired pursuant to such part of such certification or procedures shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of the United States person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

''(ii) EXCEPTION.—If the Government corrects any deficiency identified by the order of the Court under subparagraph (B), the Court may permit the use or disclosure of information obtained before the date of the correction under such minimization procedures as the Court may approve for purposes of this clause.''.

TITLE IV—FOREIGN INTELLIGENCE SURVEILLANCE COURT REFORMS

SEC. 401. APPOINTMENT OF AMICUS CURIAE.

Section 103 (50 U.S.C. 1803) is amended by adding at the end the following new subsections:

''(i) AMICUS CURIAE.—

''(1) DESIGNATION.—The presiding judges of the courts established under subsections (a) and (b) shall, not later than 180 days after the enactment of this subsection, jointly designate not fewer than 5 individuals to be eligible to serve as amicus curiae, who shall serve pursuant to rules the presiding judges may establish. In designating such individuals, the presiding judges may consider individuals recommended by any source, including members of the Privacy and Civil Liberties Oversight Board, the judges determine appropriate.

''(2) AUTHORIZATION.—A court established under subsection (a) or (b), consistent with the requirement of subsection (c) and any other statutory requirement that the court act expeditiously or within a stated time—

''(A) shall appoint an individual who has been designated under paragraph (1) to serve as amicus curiae to assist such court in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court issues a finding that such appointment is not appropriate; and

''(B) may appoint an individual or organization to serve as amicus curiae, including to provide technical expertise, in any instance as such court deems appropriate or, upon motion, permit an individual or organization leave to file an amicus curiae brief.

''(3) QUALIFICATIONS OF AMICUS CURIAE.—

''(A) EXPERTISE.—Individuals designated under paragraph (1) shall be persons who possess expertise in privacy and civil liberties, intelligence collection, communications technology, or any other area that may lend legal or technical expertise to a court established under subsection (a) or (b).

''(B) SECURITY CLEARANCE.—Individuals designated pursuant to paragraph (1) shall be persons who are determined to be eligible for access to classified information necessary to participate in matters before the courts. Amicus curiae appointed by the court pursuant to paragraph (2) shall be persons who are determined to be eligible for access to classified information, if such access is necessary to participate in the matters in which they may be appointed.

''(4) DUTIES.—If a court established under subsection (a) or (b) appoints an amicus curiae under paragraph (2)(A), the amicus curiae shall provide to the court, as appropriate—

''(A) legal arguments that advance the protection of individual privacy and civil liberties;

''(B) information related to intelligence collection or communications technology; or

''(C) legal arguments or information regarding any other area relevant to the issue presented to the court.

''(5) ASSISTANCE.—An amicus curiae appointed under paragraph (2)(A) may request that the court designate or appoint additional amici curiae pursuant to paragraph (1) or paragraph (2), to be available to assist the amicus curiae.

''(6) ACCESS TO INFORMATION.—

''(A) IN GENERAL.—If a court established under subsection (a) or (b) appoints an amicus curiae under paragraph (2), the amicus curiae—

''(i) shall have access to any legal precedent, application, certification, petition, motion, or such other materials that the court determines are relevant to the duties of the amicus curiae; and

''(ii) may, if the court determines that it is relevant to the duties of the amicus curiae, consult with any other individuals designated pursuant to paragraph (1) regarding information relevant to any assigned proceeding.

''(B) BRIEFINGS.—The Attorney General may periodically brief or provide relevant materials to individuals designated pursuant to paragraph (1) regarding constructions and interpretations of this Act and legal, technological, and other issues related to actions authorized by this Act.

''(C) CLASSIFIED INFORMATION.—An amicus curiae designated or appointed by the court may have access to classified documents, information, and other materials or proceedings only if that individual is eligible for access to classified information and to the extent consistent with the national security of the United States.

''(D) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to require the Government to provide information to an amicus curiae appointed by the court that is privileged from disclosure.

''(7) NOTIFICATION.—A presiding judge of a court established under subsection (a) or (b)

shall notify the Attorney General of each exercise of the authority to appoint an individual to serve as amicus curiae under paragraph (2).

''(8) ASSISTANCE.—A court established under subsection (a) or (b) may request and receive (including on a nonreimbursable basis) the assistance of the executive branch in the implementation of this subsection.

''(9) ADMINISTRATION.—A court established under subsection (a) or (b) may provide for the designation, appointment, removal, training, or other support for an individual designated to serve as amicus curiae under paragraph (1) or appointed to serve as amicus curiae under paragraph (2) in a manner that is not inconsistent with this subsection.

''(10) RECEIPT OF INFORMATION.—Nothing in this subsection shall limit the ability of a court established under subsection (a) or (b) to request or receive information or materials from, or otherwise communicate with, the Government or amicus curiae appointed under paragraph (2) on an ex parte basis, nor limit any special or heightened obligation in any ex parte communication or proceeding.

''(j) REVIEW OF FISA COURT DECISIONS.—Following issuance of an order under this Act, a court established under subsection (a) shall certify for review to the court established under subsection (b) any question of law that may affect resolution of the matter in controversy that the court determines warrants such review because of a need for uniformity or because consideration by the court established under subsection (b) would serve the interests of justice. Upon certification of a question of law under this subsection, the court established under subsection (b) may give binding instructions or require the entire record to be sent up for decision of the entire matter in controversy.

''(k) REVIEW OF FISA COURT OF REVIEW DECISIONS.—

''(1) CERTIFICATION.—For purposes of section 1254(2) of title 28, United States Code, the court of review established under subsection (b) shall be considered to be a court of appeals.

''(2) AMICUS CURIAE BRIEFING.—Upon certification of an application under paragraph (1), the Supreme Court of the United States may appoint an amicus curiae designated under subsection (i)(1), or any other person, to provide briefing or other assistance.''.

SEC. 402. DECLASSIFICATION OF DECISIONS, ORDERS, AND OPINIONS.

(a) DECLASSIFICATION.—Title VI (50 U.S.C. 1871 et seq.) is amended—

(1) in the heading, by striking ''**REPORTING REQUIREMENT**'' and inserting ''**OVERSIGHT**''; and

(2) by adding at the end the following new section:

''SEC. 602. DECLASSIFICATION OF SIGNIFICANT DECISIONS, ORDERS, AND OPINIONS.

''(a) DECLASSIFICATION REQUIRED.—Subject to subsection (b), the Director of National Intelligence, in consultation with the Attorney General, shall conduct a declassification review of each decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review (as defined in section 601(e)) that includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of the term 'specific selection term', and, consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion.

''(b) REDACTED FORM.—The Director of National Intelligence, in consultation with the Attorney General, may satisfy the requirement under subsection (a) to make a decision, order, or opinion described in such subsection publicly available to the greatest extent practicable by making such decision, order, or opinion publicly available in redacted form.

''(c) NATIONAL SECURITY WAIVER.—The Director of National Intelligence, in consultation with the Attorney General, may waive the requirement to declassify and make publicly available a particular decision, order, or opinion under subsection (a), if—

''(1) the Director of National Intelligence, in consultation with the Attorney General, determines that a waiver of such requirement is necessary to protect the national security of the United States or properly classified intelligence sources or methods; and

''(2) the Director of National Intelligence makes publicly available an unclassified statement prepared by the Attorney General, in consultation with the Director of National Intelligence—

''(A) summarizing the significant construction or interpretation of any provision of law, which shall include, to the extent consistent with national security, a description of the context in which the matter arises and any significant construction or interpretation of any statute, constitutional provision, or other legal authority relied on by the decision; and

''(B) that specifies that the statement has been prepared by the Attorney General and constitutes no part of the opinion of the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review.''.

(b) TABLE OF CONTENTS AMENDMENTS.—The table of contents in the first section is amended—

(1) by striking the item relating to title VI and inserting the following new item:

''TITLE VI—OVERSIGHT'';

and

(2) by inserting after the item relating to section 601 the following new item:

''Sec. 602. Declassification of significant decisions, orders, and opinions.''.

TITLE V—NATIONAL SECURITY LETTER REFORM

SEC. 501. PROHIBITION ON BULK COLLECTION.

(a) COUNTERINTELLIGENCE ACCESS TO TELEPHONE TOLL AND TRANSACTIONAL RECORDS.—Section 2709(b) of title 18, United States Code, is amended in the matter preceding paragraph (1) by striking ''may'' and inserting ''may, using a term that specifically identifies a person, entity, telephone number, or account as the basis for a request''.

(b) ACCESS TO FINANCIAL RECORDS FOR CERTAIN INTELLIGENCE AND PROTECTIVE PURPOSES.—Section 1114(a)(2) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(2)) is amended by striking the period and inserting ''and a term that specifically identifies a customer, entity, or account to be used as the basis for the production and disclosure of financial records.''.

(c) DISCLOSURES TO FBI OF CERTAIN CONSUMER RECORDS FOR COUNTERINTELLIGENCE PURPOSES.—Section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) is amended—

(1) in subsection (a), by striking ''that information,'' and inserting ''that information that includes a term that specifically identifies a consumer or account to be used as the basis for the production of that information,'';

(2) in subsection (b), by striking ''written request,'' and inserting ''written request that includes a term that specifically identifies a consumer or account to be used as the basis for the production of that information,''; and

(3) in subsection (c), by inserting '', which shall include a term that specifically identifies a consumer or account to be used as the basis for the production of the information,'' after ''issue an order ex parte''.

(d) DISCLOSURES TO GOVERNMENTAL AGENCIES FOR COUNTERTERRORISM PURPOSES OF CONSUMER REPORTS.—Section 627(a) of the Fair Credit Reporting Act (15 U.S.C. 1681v(a)) is amended by striking ''analysis.'' and inserting ''analysis and that includes a term that specifically identifies a consumer or account to be used as the basis for the production of such information.''.

SEC. 502. LIMITATIONS ON DISCLOSURE OF NATIONAL SECURITY LETTERS.

(a) COUNTERINTELLIGENCE ACCESS TO TELEPHONE TOLL AND TRANSACTIONAL RECORDS.—Section 2709 of title 18, United States Code, is amended by striking subsection (c) and inserting the following new subsection:

''(c) PROHIBITION OF CERTAIN DISCLOSURE.—

''(1) PROHIBITION.—

''(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (d) is provided, no wire or electronic communication service provider that receives a request under subsection (b), or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

''(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office, certifies that the absence of a prohibition of disclosure under this subsection may result in—

''(i) a danger to the national security of the United States;

''(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

''(iii) interference with diplomatic relations; or

''(iv) danger to the life or physical safety of any person.

''(2) EXCEPTION.—

''(A) IN GENERAL.—A wire or electronic communication service provider that receives a request under subsection (b), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

''(i) those persons to whom disclosure is necessary in order to comply with the request;

''(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

''(iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

''(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (b) in the same manner as the person to whom the request is issued.

''(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall notify the person of the applicable nondisclosure requirement.

''(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.''.

(b) ACCESS TO FINANCIAL RECORDS FOR CERTAIN INTELLIGENCE AND PROTECTIVE PURPOSES.—Section 1114 of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414) is amended—

(1) in subsection (a)(5), by striking subparagraph (D); and

(2) by inserting after subsection (b) the following new subsection:

''(c) PROHIBITION OF CERTAIN DISCLOSURE.—

''(1) PROHIBITION.—

''(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (d) is provided, no financial institution that receives a request under subsection (a), or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under subsection (a).

''(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office, certifies that the absence of a prohibition of disclosure under this subsection may result in—

''(i) a danger to the national security of the United States;

''(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

''(iii) interference with diplomatic relations; or

''(iv) danger to the life or physical safety of any person.

''(2) EXCEPTION.—

''(A) IN GENERAL.—A financial institution that receives a request under subsection (a), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

''(i) those persons to whom disclosure is necessary in order to comply with the request;

''(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

''(iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

''(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (a) in the same manner as the person to whom the request is issued.

''(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

''(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.''.

(c) IDENTITY OF FINANCIAL INSTITUTIONS AND CREDIT REPORTS.—Section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) is amended by striking subsection (d) and inserting the following new subsection:

''(d) PROHIBITION OF CERTAIN DISCLOSURE.—

''(1) PROHIBITION.—

''(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (e) is provided, no consumer reporting agency that receives a request under subsection (a) or (b) or an order under subsection (c), or officer, employee, or agent thereof, shall disclose or specify in any consumer report, that the Federal Bureau of Investigation has sought or obtained access to information or records under subsection (a), (b), or (c).

''(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office, certifies that the absence of a prohibition of disclosure under this subsection may result in—

''(i) a danger to the national security of the United States;

''(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

''(iii) interference with diplomatic relations; or

''(iv) danger to the life or physical safety of any person.

''(2) EXCEPTION.—

''(A) IN GENERAL.—A consumer reporting agency that receives a request under subsection (a) or (b) or an order under subsection (c), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

''(i) those persons to whom disclosure is necessary in order to comply with the request;

''(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

''(iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

''(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request under subsection (a) or (b) or an order under subsection (c) is issued in the same manner as the person to whom the request is issued.

''(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

''(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.''.

(d) CONSUMER REPORTS.—Section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v) is amended by striking subsection (c) and inserting the following new subsection:

''(c) PROHIBITION OF CERTAIN DISCLOSURE.—

''(1) PROHIBITION.—

''(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (d) is provided, no consumer reporting agency that receives a request under subsection (a), or officer, employee, or agent thereof, shall disclose or specify in any consumer report, that a government agency described in subsection (a) has sought or obtained access to information or records under subsection (a).

''(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the head of the government agency described in subsection (a), or a designee, certifies that the absence of a prohibition of disclosure under this subsection may result in—

''(i) a danger to the national security of the United States;

''(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

''(iii) interference with diplomatic relations; or

''(iv) danger to the life or physical safety of any person.

''(2) EXCEPTION.—

''(A) IN GENERAL.—A consumer reporting agency that receives a request under subsection (a), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

''(i) those persons to whom disclosure is necessary in order to comply with the request;

''(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

''(iii) other persons as permitted by the head of the government agency described in subsection (a) or a designee.

''(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request under subsection (a) is issued in the same manner as the person to whom the request is issued.

''(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

''(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the head of the government agency described in subsection (a) or a designee, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the head or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.''.

(e) INVESTIGATIONS OF PERSONS WITH ACCESS TO CLASSIFIED INFORMATION.—Section 802 of the National Security Act of 1947 (50 U.S.C. 3162) is amended by striking subsection (b) and inserting the following new subsection:

''(b) PROHIBITION OF CERTAIN DISCLOSURE.—

''(1) PROHIBITION.—

''(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (c) is provided, no governmental or private entity that receives a request under subsection (a), or officer, employee, or agent thereof, shall disclose to any person that an authorized investigative agency described in subsection (a) has sought or obtained access to information under subsection (a).

''(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the head of an authorized investigative agency described in subsection (a), or a designee, certifies that the absence of a prohibition of disclosure under this subsection may result in—

''(i) a danger to the national security of the United States;

''(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

''(iii) interference with diplomatic relations; or

''(iv) danger to the life or physical safety of any person.

''(2) EXCEPTION.—

''(A) IN GENERAL.—A governmental or private entity that receives a request under subsection (a), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

''(i) those persons to whom disclosure is necessary in order to comply with the request;

''(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

''(iii) other persons as permitted by the head of the authorized investigative agency described in subsection (a) or a designee.

''(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (a) in the same manner as the person to whom the request is issued.

''(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

''(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the head of an authorized investigative agency described in subsection (a), or a designee, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the head of the authorized investigative agency or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.''.

(f) TERMINATION PROCEDURES.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Attorney General shall adopt procedures with respect to nondisclosure requirements issued pursuant to section 2709 of title 18, United States Code, section 626 or 627 of the Fair Credit Reporting Act (15 U.S.C. 1681u and 1681v), section 1114 of the Right to Financial Privacy Act (12 U.S.C. 3414), or section 802 of the National Security Act of 1947 (50 U.S.C. 3162), as amended by this Act, to require—

(A) the review at appropriate intervals of such a nondisclosure requirement to assess whether the facts supporting nondisclosure continue to exist;

(B) the termination of such a nondisclosure requirement if the facts no longer support nondisclosure; and

(C) appropriate notice to the recipient of the national security letter, or officer, employee, or agent thereof, subject to the nondisclosure requirement, and the applicable court as appropriate, that the nondisclosure requirement has been terminated.

(2) REPORTING.—Upon adopting the procedures required under paragraph (1), the Attorney General shall submit the procedures to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives.

(g) JUDICIAL REVIEW.—Section 3511 of title 18, United States Code, is amended by striking subsection (b) and inserting the following new subsection:

''(b) NONDISCLOSURE.—

''(1) IN GENERAL.—

''(A) NOTICE.—If a recipient of a request or order for a report, records, or other information under section 2709 of this title, section 626 or 627 of the Fair Credit Reporting Act (15 U.S.C. 1681u and 1681v), section 1114 of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414), or section 802 of the National Security Act of 1947 (50 U.S.C. 3162), wishes to have a court review a nondisclosure requirement imposed in connection with the request or order, the recipient may notify the Government or file a petition for judicial review in any court described in subsection (a).

''(B) APPLICATION.—Not later than 30 days after the date of receipt of a notification under subparagraph (A), the Government shall apply for an order prohibiting the disclosure of the existence or contents of the relevant request or order. An application under this subparagraph may be filed in the district court of the United States for the judicial district in which the recipient of the order is doing business or in the district court of the United States for any judicial district within which the authorized investigation that is the basis for the request is being conducted. The applicable nondisclosure requirement shall remain in effect during the pendency of proceedings relating to the requirement.

''(C) CONSIDERATION.—A district court of the United States that receives a petition under subparagraph (A) or an application under subparagraph (B) should rule expeditiously, and shall, subject to paragraph (3), issue a nondisclosure order that includes conditions appropriate to the circumstances.

''(2) APPLICATION CONTENTS.—An application for a nondisclosure order or extension thereof or a response to a petition filed under paragraph (1) shall include a certification from the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation, or a designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, or in the case of a request by a department, agency, or instrumentality of the Federal Government other than the Department of Justice, the head or deputy head of the department, agency, or instrumentality, containing a statement of specific facts indicating that the absence of a prohibition of disclosure under this subsection may result in—

''(A) a danger to the national security of the United States;

''(B) interference with a criminal, counterterrorism, or counterintelligence investigation;

''(C) interference with diplomatic relations; or

''(D) danger to the life or physical safety of any person.

''(3) STANDARD.—A district court of the United States shall issue a nondisclosure order or extension thereof under this subsection if the court determines that there is reason to believe that disclosure of the information subject to the nondisclosure requirement during the applicable time period may result in—

''(A) a danger to the national security of the United States;

''(B) interference with a criminal, counterterrorism, or counterintelligence investigation;

''(C) interference with diplomatic relations; or

''(D) danger to the life or physical safety of any person.''.

SEC. 503. JUDICIAL REVIEW.

(a) COUNTERINTELLIGENCE ACCESS TO TELEPHONE TOLL AND TRANSACTIONAL RECORDS.—Section 2709 of title 18, United States Code, is amended—

(1) by redesignating subsections (d), (e), and (f) as subsections (e), (f), and (g), respectively; and

(2) by inserting after subsection (c) the following new subsection:

''(d) JUDICIAL REVIEW.—

''(1) IN GENERAL.—A request under subsection (b) or a nondisclosure requirement imposed in connection with such request under subsection (c) shall be subject to judicial review under section 3511.

''(2) NOTICE.—A request under subsection (b) shall include notice of the availability of judicial review described in paragraph (1).''.

(b) ACCESS TO FINANCIAL RECORDS FOR CERTAIN INTELLIGENCE AND PROTECTIVE PURPOSES.—Section 1114 of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414) is amended—

(1) by redesignating subsection (d) as subsection (e); and

(2) by inserting after subsection (c) the following new subsection:

''(d) JUDICIAL REVIEW.—

''(1) IN GENERAL.—A request under subsection (a) or a nondisclosure requirement imposed in connection with such request under subsection (c) shall be subject to judicial review under section 3511 of title 18, United States Code.

''(2) NOTICE.—A request under subsection (a) shall include notice of the availability of judicial review described in paragraph (1).''.

(c) IDENTITY OF FINANCIAL INSTITUTIONS AND CREDIT REPORTS.—Section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) is amended—

(1) by redesignating subsections (e) through (m) as subsections (f) through (n), respectively; and

(2) by inserting after subsection (d) the following new subsection:

''(e) JUDICIAL REVIEW.—

''(1) IN GENERAL.—A request under subsection (a) or (b) or an order under subsection (c) or a non-disclosure requirement imposed in connection with such request under subsection (d) shall be subject to judicial review under section 3511 of title 18, United States Code.

''(2) NOTICE.—A request under subsection (a) or (b) or an order under subsection (c) shall include notice of the availability of judicial review described in paragraph (1).''.

(d) IDENTITY OF FINANCIAL INSTITUTIONS AND CREDIT REPORTS.—Section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v) is amended—

(1) by redesignating subsections (d), (e), and (f) as subsections (e), (f), and (g), respectively; and

(2) by inserting after subsection (c) the following new subsection:

''(d) JUDICIAL REVIEW.—

''(1) IN GENERAL.—A request under subsection (a) or a non-disclosure requirement imposed in connection with such request under subsection (c) shall be subject to judicial review under section 3511 of title 18, United States Code.

''(2) NOTICE.—A request under subsection (a) shall include notice of the availability of judicial review described in paragraph (1).''.

(e) INVESTIGATIONS OF PERSONS WITH ACCESS TO CLASSIFIED INFORMATION.—Section 802 of the National Security Act of 1947 (50 U.S.C. 3162) is amended—

(1) by redesignating subsections (c) through (f) as subsections (d) through (g), respectively; and

(2) by inserting after subsection (b) the following new subsection:

''(c) JUDICIAL REVIEW.—

''(1) IN GENERAL.—A request under subsection (a) or a nondisclosure requirement imposed in connection with such request under subsection (b) shall be subject to judicial review under section 3511 of title 18, United States Code.

''(2) NOTICE.—A request under subsection (a) shall include notice of the availability of judicial review described in paragraph (1).''.

TITLE VI—FISA TRANSPARENCY AND REPORTING REQUIREMENTS

SEC. 601. ADDITIONAL REPORTING ON ORDERS REQUIRING PRODUCTION OF BUSINESS RECORDS; BUSINESS RECORDS COMPLIANCE REPORTS TO CONGRESS.

(a) REPORTS SUBMITTED TO COMMITTEES.—Section 502(b) (50 U.S.C. 1862(b)) is amended—

(1) by redesignating paragraphs (1), (2), and (3) as paragraphs (6), (7), and (8), respectively; and

(2) by inserting before paragraph (6) (as so redesignated) the following new paragraphs:

''(1) a summary of all compliance reviews conducted by the Government for the production of tangible things under section 501;

''(2) the total number of applications described in section 501(b)(2)(B) made for orders approving requests for the production of tangible things;

''(3) the total number of such orders either granted, modified, or denied;

''(4) the total number of applications described in section 501(b)(2)(C) made for orders approving requests for the production of call detail records;

''(5) the total number of such orders either granted, modified, or denied;''.

(b) REPORTING ON CERTAIN TYPES OF PRODUCTION.—Section 502(c)(1) (50 U.S.C. 1862(c)(1)) is amended—

(1) in subparagraph (A), by striking ''and'';

(2) in subparagraph (B), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following new subparagraphs:

''(C) the total number of applications made for orders approving requests for the production of tangible things under section 501 in which the specific selection term does not specifically identify an individual, account, or personal device;

''(D) the total number of orders described in subparagraph (C) either granted, modified, or denied; and

''(E) with respect to orders described in subparagraph (D) that have been granted or modified, whether the court established under section 103 has directed additional, particularized minimization procedures beyond those adopted pursuant to section 501(g).''.

SEC. 602. ANNUAL REPORTS BY THE GOVERNMENT.

(a) IN GENERAL.—Title VI (50 U.S.C. 1871 et seq.), as amended by section 402 of this Act, is further amended by adding at the end the following new section:

''SEC. 603. ANNUAL REPORTS.

''(a) REPORT BY DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS.—

''(1) REPORT REQUIRED.—The Director of the Administrative Office of the United States Courts shall annually submit to the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate, subject to a declassification review by the Attorney General and the Director of National Intelligence, a report that includes—

''(A) the number of applications or certifications for orders submitted under each of sections 105, 304, 402, 501, 702, 703, and 704;

''(B) the number of such orders granted under each of those sections;

''(C) the number of orders modified under each of those sections;

''(D) the number of applications or certifications denied under each of those sections;

''(E) the number of appointments of an individual to serve as amicus curiae under section 103, including the name of each individual appointed to serve as amicus curiae; and

''(F) the number of findings issued under section 103(i) that such appointment is not appropriate and the text of any such findings.

''(2) PUBLICATION.—The Director shall make the report required under paragraph (1) publicly available on an Internet Web site, except that the Director shall not make publicly available on an Internet Web site the findings described in subparagraph (F) of paragraph (1).

''(b) MANDATORY REPORTING BY DIRECTOR OF NATIONAL INTELLIGENCE.—Except as provided in subsection (d), the Director of National Intelligence shall annually make publicly available on an Internet Web site a report that identifies, for the preceding 12-month period—

''(1) the total number of orders issued pursuant to titles I and III and sections 703 and 704 and a good faith estimate of the number of targets of such orders;

''(2) the total number of orders issued pursuant to section 702 and a good faith estimate of—

''(A) the number of search terms concerning a known United States person used to retrieve the unminimized contents of electronic communications or wire communications obtained through acquisitions authorized under such section, excluding the number of search terms used to prevent the return of information concerning a United States person; and

''(B) the number of queries concerning a known United States person of unminimized noncontents information relating to electronic communications or wire communications obtained through acquisitions authorized under such section, excluding the number of queries containing information used to prevent the return of information concerning a United States person;

''(3) the total number of orders issued pursuant to title IV and a good faith estimate of—

''(A) the number of targets of such orders; and

''(B) the number of unique identifiers used to communicate information collected pursuant to such orders;

''(4) the total number of orders issued pursuant to applications made under section 501(b)(2)(B) and a good faith estimate of—

''(A) the number of targets of such orders; and

''(B) the number of unique identifiers used to communicate information collected pursuant to such orders;

''(5) the total number of orders issued pursuant to applications made under section 501(b)(2)(C) and a good faith estimate of—

''(A) the number of targets of such orders;

''(B) the number of unique identifiers used to communicate information collected pursuant to such orders; and

''(C) the number of search terms that included information concerning a United States person that were used to query any database of call detail records obtained through the use of such orders; and

''(6) the total number of national security letters issued and the number of requests for information contained within such national security letters.

''(c) TIMING.—The annual reports required by subsections (a) and (b) shall be made publicly available during April of each year and include information relating to the previous calendar year.

''(d) EXCEPTIONS.—

''(1) STATEMENT OF NUMERICAL RANGE.—If a good faith estimate required to be reported under subparagraph (B) of any of paragraphs (3), (4), or (5) of subsection (b) is fewer than 500, it shall be expressed as a numerical range of 'fewer than 500' and shall not be expressed as an individual number.

''(2) NONAPPLICABILITY TO CERTAIN INFORMATION.—

''(A) FEDERAL BUREAU OF INVESTIGATION.—Paragraphs (2)(A), (2)(B), and (5)(C) of subsection (b) shall not apply to information or records held by, or queries conducted by, the Federal Bureau of Investigation.

''(B) ELECTRONIC MAIL ADDRESS AND TELEPHONE NUMBERS.—Paragraph (3)(B) of subsection (b) shall not apply to orders resulting in the acquisition of information by the Federal Bureau of Investigation that does not include electronic mail addresses or telephone numbers.

''(3) CERTIFICATION.—

''(A) IN GENERAL.—If the Director of National Intelligence concludes that a good faith estimate required to be reported under subsection (b)(2)(B) cannot be determined accurately because some but not all of the relevant elements of the intelligence community are able to provide such good faith estimate, the Director shall—

''(i) certify that conclusion in writing to the Select Committee on Intelligence and the Committee on the Judiciary of the Senate and the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives;

''(ii) report the good faith estimate for those relevant elements able to provide such good faith estimate;

''(iii) explain when it is reasonably anticipated that such an estimate will be able to be determined fully and accurately; and

''(iv) make such certification publicly available on an Internet Web site.

''(B) FORM.—A certification described in subparagraph (A) shall be prepared in unclassified form, but may contain a classified annex.

''(C) TIMING.—If the Director of National Intelligence continues to conclude that the good faith estimates described in this paragraph cannot be determined accurately, the Director shall annually submit a certification in accordance with this paragraph.

''(e) DEFINITIONS.—In this section:

''(1) CONTENTS.—The term 'contents' has the meaning given that term under section 2510 of title 18, United States Code.

''(2) ELECTRONIC COMMUNICATION.—The term 'electronic communication' has the meaning given that term under section 2510 of title 18, United States Code.

''(3) NATIONAL SECURITY LETTER.—The term 'national security letter' means a request for a report, records, or other information under—

''(A) section 2709 of title 18, United States Code;

''(B) section 1114(a)(5)(A) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(5)(A));

''(C) subsection (a) or (b) of section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u(a), 1681u(b)); or

''(D) section 627(a) of the Fair Credit Reporting Act (15 U.S.C. 1681v(a)).

''(4) UNITED STATES PERSON.—The term 'United States person' means a citizen of the United States or an alien lawfully admitted for permanent residence (as defined in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a))).

''(5) WIRE COMMUNICATION.—The term 'wire communication' has the meaning given that term under section 2510 of title 18, United States Code.''.

(b) TABLE OF CONTENTS AMENDMENT.—The table of contents, as amended by section 402 of this Act, is further amended by inserting after the item relating to section 602, as added by section 402 of this Act, the following new item:

''Sec. 603. Annual reports.''.

(c) PUBLIC REPORTING ON NATIONAL SECURITY LETTERS.—Section 118(c) of the USA PATRIOT Improvement and Reauthorization Act of 2005 (18 U.S.C. 3511 note) is amended—

(1) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking ''United States''; and

(B) in subparagraph (A), by striking '', excluding the number of requests for subscriber information'';

(2) by redesignating paragraph (2) as paragraph (3); and

(3) by inserting after paragraph (1) the following:

''(2) CONTENT.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), each report required under this subsection shall include a good faith estimate of the total number of requests described in paragraph (1) requiring disclosure of information concerning—

''(i) United States persons; and

''(ii) persons who are not United States persons.

''(B) EXCEPTION.—With respect to the number of requests for subscriber information under section 2709 of title 18, United States Code, a report required under this subsection need not separate the number of requests into each of the categories described in subparagraph (A).''.

(d) STORED COMMUNICATIONS.—Section 2702(d) of title 18, United States Code, is amended—

(1) in paragraph (1), by striking ''; and'' and inserting a semicolon;

(2) in paragraph (2)(B), by striking the period and inserting ''; and''; and

(3) by adding at the end the following new paragraph:

''(3) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (c)(4).''.

SEC. 603. PUBLIC REPORTING BY PERSONS SUBJECT TO FISA ORDERS.

(a) IN GENERAL.—Title VI (50 U.S.C. 1871 et seq.), as amended by sections 402 and 602 of this Act, is further amended by adding at the end the following new section:

''SEC. 604. PUBLIC REPORTING BY PERSONS SUBJECT TO ORDERS.

''(a) REPORTING.—A person subject to a nondisclosure requirement accompanying an order or directive under this Act or a national security letter may, with respect to such order, directive, or national security letter, publicly report the following information using one of the following structures:

''(1) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply into separate categories of—

''(A) the number of national security letters received, reported in bands of 1000 starting with 0–999;

''(B) the number of customer selectors targeted by national security letters, reported in bands of 1000 starting with 0–999;

''(C) the number of orders or directives received, combined, under this Act for contents, reported in bands of 1000 starting with 0–999;

''(D) the number of customer selectors targeted under orders or directives received, combined, under this Act for contents reported in bands of 1000 starting with 0–999;

''(E) the number of orders received under this Act for noncontents, reported in bands of 1000 starting with 0–999; and

''(F) the number of customer selectors targeted under orders under this Act for noncontents, reported in bands of 1000 starting with 0–999, pursuant to—

''(i) title IV;

''(ii) title V with respect to applications described in section 501(b)(2)(B); and

''(iii) title V with respect to applications described in section 501(b)(2)(C).

''(2) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply into separate categories of—

''(A) the number of national security letters received, reported in bands of 500 starting with 0–499;

''(B) the number of customer selectors targeted by national security letters, reported in bands of 500 starting with 0–499;

''(C) the number of orders or directives received, combined, under this Act for contents, reported in bands of 500 starting with 0–499;

''(D) the number of customer selectors targeted under orders or directives received, combined, under this Act for contents, reported in bands of 500 starting with 0–499;

''(E) the number of orders received under this Act for noncontents, reported in bands of 500 starting with 0–499; and

''(F) the number of customer selectors targeted under orders received under this Act for noncontents, reported in bands of 500 starting with 0–499.

''(3) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply in the into separate categories of—

''(A) the total number of all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 250 starting with 0–249; and

''(B) the total number of customer selectors targeted under all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 250 starting with 0–249.

''(4) An annual report that aggregates the number of orders, directives, and national security letters the person was required to comply with into separate categories of—

''(A) the total number of all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 100 starting with 0–99; and

''(B) the total number of customer selectors targeted under all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 100 starting with 0–99.

''(b) PERIOD OF TIME COVERED BY REPORTS.—

''(1) A report described in paragraph (1) or (2) of subsection (a) shall include only information—

''(A) relating to national security letters for the previous 180 days; and

''(B) relating to authorities under this Act for the 180-day period of time ending on the date that is not less than 180 days prior to the date of the publication of such report, except that with respect to a platform, product, or service for which a person did not previously receive an order or directive (not including an enhancement to or iteration of an existing publicly available platform, product, or service) such report shall not include any information relating to such new order or directive until 540 days after the date on which such new order or directive is received.

''(2) A report described in paragraph (3) of subsection (a) shall include only information relating to the previous 180 days.

''(3) A report described in paragraph (4) of subsection (a) shall include only information for the 1-year period of time ending on the date that is not less than 1 year prior to the date of the publication of such report.

''(c) OTHER FORMS OF AGREED TO PUBLICATION.—Nothing in this section prohibits the Government and any person from jointly agreeing to the publication of information referred to in this subsection in a time, form, or manner other than as described in this section.

''(d) DEFINITIONS.—In this section:

''(1) CONTENTS.—The term 'contents' has the meaning given that term under section 2510 of title 18, United States Code.

''(2) NATIONAL SECURITY LETTER.—The term 'national security letter' has the meaning given that term under section 603.''.

(b) TABLE OF CONTENTS AMENDMENT.—The table of contents, as amended by sections 402 and 602 of this Act, is further amended by inserting after the item relating to section 603, as added by section 602 of this Act, the following new item:

''Sec. 604. Public reporting by persons subject to orders.''.

SEC. 604. REPORTING REQUIREMENTS FOR DECISIONS, ORDERS, AND OPINIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT AND THE FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW.

Section 601(c)(1) (50 U.S.C. 1871(c)(1)) is amended to read as follows:

''(1) not later than 45 days after the date on which the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review issues a decision, order, or opinion, including any denial or modification of an application under this Act, that includes significant construction or interpretation of any provision of law or results in a change of application of any provision of this Act or a novel application of any provision of this Act, a copy of such decision, order, or opinion and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion; and''.

SEC. 605. SUBMISSION OF REPORTS UNDER FISA.

(a) ELECTRONIC SURVEILLANCE.—Section 108(a)(1) (50 U.S.C. 1808(a)(1)) is amended by striking ''the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, and the Committee on the Judiciary of the Senate,'' and inserting ''the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate''.

(b) PHYSICAL SEARCHES.—The matter preceding paragraph (1) of section 306 (50 U.S.C. 1826) is amended—

(1) in the first sentence, by striking ''Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the Senate,'' and inserting ''Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate''; and

(2) in the second sentence, by striking ''and the Committee on the Judiciary of the House of Representatives''.

(c) PEN REGISTERS AND TRAP AND TRACE DEVICES.—Section 406(b) (50 U.S.C. 1846(b)) is amended—

(1) in paragraph (2), by striking ''; and'' and inserting a semicolon;

(2) in paragraph (3), by striking the period and inserting a semicolon; and

(3) by adding at the end the following new paragraphs:

''(4) each department or agency on behalf of which the Attorney General or a designated attorney for the Government has made an application for an order authorizing or approving the installation and use of a pen register or trap and trace device under this title; and

''(5) for each department or agency described in paragraph (4), each number described in paragraphs (1), (2), and (3).''.

(d) ACCESS TO CERTAIN BUSINESS RECORDS AND OTHER TANGIBLE THINGS.—Section 502(a) (50 U.S.C. 1862(a)) is amended by striking ''Permanent Select Committee on Intelligence of the House of Representatives and

the Select Committee on Intelligence and the Committee on the Judiciary of the Senate'' and inserting ''Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate''.

TITLE VII—ENHANCED NATIONAL SECURITY PROVISIONS

SEC. 701. EMERGENCIES INVOLVING NON-UNITED STATES PERSONS.

(a) IN GENERAL.—Section 105 (50 U.S.C. 1805) is amended—

(1) by redesignating subsections (f), (g), (h), and (i) as subsections (g), (h), (i), and (j), respectively; and

(2) by inserting after subsection (e) the following:

''(f)(1) Notwithstanding any other provision of this Act, the lawfully authorized targeting of a non-United States person previously believed to be located outside the United States for the acquisition of foreign intelligence information may continue for a period not to exceed 72 hours from the time that the non-United States person is reasonably believed to be located inside the United States and the acquisition is subject to this title or to title III of this Act, provided that the head of an element of the intelligence community—

''(A) reasonably determines that a lapse in the targeting of such non-United States person poses a threat of death or serious bodily harm to any person;

''(B) promptly notifies the Attorney General of a determination under subparagraph (A); and

''(C) requests, as soon as practicable, the employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical search pursuant to section 304(e), as warranted.

''(2) The authority under this subsection to continue the acquisition of foreign intelligence information is limited to a period not to exceed 72 hours and shall cease upon the earlier of the following:

''(A) The employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical search pursuant to section 304(e).

''(B) An issuance of a court order under this title or title III of this Act.

''(C) The Attorney General provides direction that the acquisition be terminated.

''(D) The head of the element of the intelligence community conducting the acquisition determines that a request under paragraph (1)(C) is not warranted.

''(E) When the threat of death or serious bodily harm to any person is no longer reasonably believed to exist.

''(3) Nonpublicly available information concerning unconsenting United States persons acquired under this subsection shall not be disseminated during the 72 hour time period under paragraph (1) unless necessary to investigate, reduce, or eliminate the threat of death or serious bodily harm to any person.

''(4) If the Attorney General declines to authorize the employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical search pursuant to section 304(e), or a court order is not obtained under this title or title III of this Act, information obtained during the 72 hour acquisition time period under paragraph (1) shall not be retained, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

''(5) Paragraphs (5) and (6) of subsection (e) shall apply to this subsection.''.

(b) NOTIFICATION OF EMERGENCY EMPLOYMENT OF ELECTRONIC SURVEILLANCE.—Section 106(j) (50 U.S.C. 1806(j)) is amended by striking ''section 105(e)'' and inserting ''subsection (e) or (f) of section 105''.

(c) REPORT TO CONGRESS.—Section 108(a)(2) (50 U.S.C. 1808(a)(2)) is amended—

(1) in subparagraph (B), by striking ''and'' at the end;

(2) in subparagraph (C), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following:

''(D) the total number of authorizations under section 105(f) and the total number of subsequent emergency employments of electronic surveillance under section 105(e) or emergency physical searches pursuant to section 301(e).''.

SEC. 702. PRESERVATION OF TREATMENT OF NON-UNITED STATES PERSONS TRAVELING OUTSIDE THE UNITED STATES AS AGENTS OF FOREIGN POWERS.

Section 101(b)(1) is amended—

(1) in subparagraph (A), by inserting before the semicolon at the end the following: '', irrespective of whether the person is inside the United States''; and

(2) in subparagraph (B)—

(A) by striking ''of such person's presence in the United States''; and

(B) by striking ''such activities in the United States'' and inserting ''such activities''.

SEC. 703. IMPROVEMENT TO INVESTIGATIONS OF INTERNATIONAL PROLIFERATION OF WEAPONS OF MASS DESTRUCTION.

Section 101(b)(1) is further amended by striking subparagraph (E) and inserting the following new subparagraph (E):

''(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power, or knowingly aids or abets any person in the conduct of such proliferation or activities in preparation therefor, or knowingly conspires with any person to engage in such proliferation or activities in preparation therefor; or''.

SEC. 704. INCREASE IN PENALTIES FOR MATERIAL SUPPORT OF FOREIGN TERRORIST ORGANIZATIONS.

Section 2339B(a)(1) of title 18, United States Code, is amended by striking ''15 years'' and inserting ''20 years''.

SEC. 705. SUNSETS.

(a) USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT OF 2005.—Section 102(b)(1) of the USA PATRIOT Improvement and Reauthorization Act of 2005 (50 U.S.C. 1805 note) is amended by striking ''June 1, 2015'' and inserting ''December 15, 2019''.

(b) INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004.—Section 6001(b)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 1801 note) is amended by striking ''June 1, 2015'' and inserting ''December 15, 2019''.

(c) CONFORMING AMENDMENT.—Section 102(b)(1) of the USA PATRIOT Improvement and Reauthorization Act of 2005 (50 U.S.C. 1805 note), as amended by subsection (a), is further amended by striking ''sections 501, 502, and'' and inserting ''title V and section''.

TITLE VIII—SAFETY OF MARITIME NAVIGATION AND NUCLEAR TERRORISM CONVENTIONS IMPLEMENTATION

Subtitle A—Safety of Maritime Navigation

SEC. 801. AMENDMENT TO SECTION 2280 OF TITLE 18, UNITED STATES CODE.

Section 2280 of title 18, United States Code, is amended—

(1) in subsection (b)—

(A) in paragraph (1)(A)(i), by striking ''a ship flying the flag of the United States'' and inserting ''a vessel of the United States or a vessel subject to the jurisdiction of the United States (as defined in section 70502 of title 46)'';

(B) in paragraph (1)(A)(ii), by inserting '', including the territorial seas'' after ''in the United States''; and

(C) in paragraph (1)(A)(iii), by inserting '', by a United States corporation or legal entity,'' after ''by a national of the United States'';

(2) in subsection (c), by striking ''section 2(c)'' and inserting ''section 13(c)'';

(3) by striking subsection (d);

(4) by striking subsection (e) and inserting after subsection (c) the following:

''(d) DEFINITIONS.—As used in this section, section 2280a, section 2281, and section 2281a, the term—

''(1) 'applicable treaty' means—

''(A) the Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16 December 1970;

''(B) the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 23 September 1971;

''(C) the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on 14 December 1973;

''(D) International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on 17 December 1979;

''(E) the Convention on the Physical Protection of Nuclear Material, done at Vienna on 26 October 1979;

''(F) the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 24 February 1988;

''(G) the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, done at Rome on 10 March 1988;

''(H) International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997; and

''(I) International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations on 9 December 1999;

''(2) 'armed conflict' does not include internal disturbances and tensions, such as riots, isolated and sporadic acts of violence, and other acts of a similar nature;

''(3) 'biological weapon' means—

''(A) microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective, or other peaceful purposes; or

''(B) weapons, equipment, or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict;

''(4) 'chemical weapon' means, together or separately—

''(A) toxic chemicals and their precursors, except where intended for—

''(i) industrial, agricultural, research, medical, pharmaceutical, or other peaceful purposes;

''(ii) protective purposes, namely those purposes directly related to protection against toxic chemicals and to protection against chemical weapons;

''(iii) military purposes not connected with the use of chemical weapons and not dependent on the use of the toxic properties of chemicals as a method of warfare; or

''(iv) law enforcement including domestic riot control purposes,

as long as the types and quantities are consistent with such purposes;

''(B) munitions and devices, specifically designed to cause death or other harm through

the toxic properties of those toxic chemicals specified in subparagraph (A), which would be released as a result of the employment of such munitions and devices; and

''(C) any equipment specifically designed for use directly in connection with the employment of munitions and devices specified in subparagraph (B);

''(5) 'covered ship' means a ship that is navigating or is scheduled to navigate into, through or from waters beyond the outer limit of the territorial sea of a single country or a lateral limit of that country's territorial sea with an adjacent country;

''(6) 'explosive material' has the meaning given the term in section 841(c) and includes explosive as defined in section 844(j) of this title;

''(7) 'infrastructure facility' has the meaning given the term in section 2332f(e)(5) of this title;

''(8) 'international organization' has the meaning given the term in section 831(f)(3) of this title;

''(9) 'military forces of a state' means the armed forces of a state which are organized, trained, and equipped under its internal law for the primary purpose of national defense or security, and persons acting in support of those armed forces who are under their formal command, control, and responsibility;

''(10) 'national of the United States' has the meaning stated in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22));

''(11) 'Non-Proliferation Treaty' means the Treaty on the Non-Proliferation of Nuclear Weapons, done at Washington, London, and Moscow on 1 July 1968;

''(12) 'Non-Proliferation Treaty State Party' means any State Party to the Non-Proliferation Treaty, to include Taiwan, which shall be considered to have the obligations under the Non-Proliferation Treaty of a party to that treaty other than a Nuclear Weapon State Party to the Non-Proliferation Treaty;

''(13) 'Nuclear Weapon State Party to the Non-Proliferation Treaty' means a State Party to the Non-Proliferation Treaty that is a nuclear-weapon State, as that term is defined in Article IX(3) of the Non-Proliferation Treaty;

''(14) 'place of public use' has the meaning given the term in section 2332f(e)(6) of this title;

''(15) 'precursor' has the meaning given the term in section 229F(6)(A) of this title;

''(16) 'public transport system' has the meaning given the term in section 2332f(e)(7) of this title;

''(17) 'serious injury or damage' means—

''(A) serious bodily injury,

''(B) extensive destruction of a place of public use, State or government facility, infrastructure facility, or public transportation system, resulting in major economic loss, or

''(C) substantial damage to the environment, including air, soil, water, fauna, or flora;

''(18) 'ship' means a vessel of any type whatsoever not permanently attached to the sea-bed, including dynamically supported craft, submersibles, or any other floating craft, but does not include a warship, a ship owned or operated by a government when being used as a naval auxiliary or for customs or police purposes, or a ship which has been withdrawn from navigation or laid up;

''(19) 'source material' has the meaning given that term in the International Atomic Energy Agency Statute, done at New York on 26 October 1956;

''(20) 'special fissionable material' has the meaning given that term in the International Atomic Energy Agency Statute, done at New York on 26 October 1956;

''(21) 'territorial sea of the United States' means all waters extending seaward to 12 nautical miles from the baselines of the United States determined in accordance with international law;

''(22) 'toxic chemical' has the meaning given the term in section 229F(8)(A) of this title;

''(23) 'transport' means to initiate, arrange or exercise effective control, including decisionmaking authority, over the movement of a person or item; and

''(24) 'United States', when used in a geographical sense, includes the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, and all territories and possessions of the United States.''; and

(5) by inserting after subsection (d) (as added by paragraph (4) of this section) the following:

''(e) EXCEPTIONS.—This section shall not apply to—

''(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

''(2) activities undertaken by military forces of a state in the exercise of their official duties.

''(f) DELIVERY OF SUSPECTED OFFENDER.—The master of a covered ship flying the flag of the United States who has reasonable grounds to believe that there is on board that ship any person who has committed an offense under section 2280 or section 2280a may deliver such person to the authorities of a country that is a party to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation. Before delivering such person to the authorities of another country, the master shall notify in an appropriate manner the Attorney General of the United States of the alleged offense and await instructions from the Attorney General as to what action to take. When delivering the person to a country which is a state party to the Convention, the master shall, whenever practicable, and if possible before entering the territorial sea of such country, notify the authorities of such country of the master's intention to deliver such person and the reasons therefor. If the master delivers such person, the master shall furnish to the authorities of such country the evidence in the master's possession that pertains to the alleged offense.

''(g)(1) CIVIL FORFEITURE.—Any real or personal property used or intended to be used to commit or to facilitate the commission of a violation of this section, the gross proceeds of such violation, and any real or personal property traceable to such property or proceeds, shall be subject to forfeiture.

''(2) APPLICABLE PROCEDURES.—Seizures and forfeitures under this section shall be governed by the provisions of chapter 46 of title 18, United States Code, relating to civil forfeitures, except that such duties as are imposed upon the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents, and other persons as may be designated for that purpose by the Secretary of Homeland Security, the Attorney General, or the Secretary of Defense.''.

SEC. 802. NEW SECTION 2280A OF TITLE 18, UNITED STATES CODE.

(a) IN GENERAL.—Chapter 111 of title 18, United States Code, is amended by adding after section 2280 the following new section:

''§ 2280a. Violence against maritime navigation and maritime transport involving weapons of mass destruction

''(a) OFFENSES.—

''(1) IN GENERAL.—Subject to the exceptions in subsection (c), a person who unlawfully and intentionally—

''(A) when the purpose of the act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act—

''(i) uses against or on a ship or discharges from a ship any explosive or radioactive material, biological, chemical, or nuclear weapon or other nuclear explosive device in a manner that causes or is likely to cause death to any person or serious injury or damage;

''(ii) discharges from a ship oil, liquefied natural gas, or another hazardous or noxious substance that is not covered by clause (i), in such quantity or concentration that causes or is likely to cause death to any person or serious injury or damage; or

''(iii) uses a ship in a manner that causes death to any person or serious injury or damage;

''(B) transports on board a ship—

''(i) any explosive or radioactive material, knowing that it is intended to be used to cause, or in a threat to cause, death to any person or serious injury or damage for the purpose of intimidating a population, or compelling a government or an international organization to do or to abstain from doing any act;

''(ii) any biological, chemical, or nuclear weapon or other nuclear explosive device, knowing it to be a biological, chemical, or nuclear weapon or other nuclear explosive device;

''(iii) any source material, special fissionable material, or equipment or material especially designed or prepared for the processing, use, or production of special fissionable material, knowing that it is intended to be used in a nuclear explosive activity or in any other nuclear activity not under safeguards pursuant to an International Atomic Energy Agency comprehensive safeguards agreement, except where—

''(I) such item is transported to or from the territory of, or otherwise under the control of, a Non-Proliferation Treaty State Party; and

''(II) the resulting transfer or receipt (including internal to a country) is not contrary to the obligations under the Non-Proliferation Treaty of the Non-Proliferation Treaty State Party from which, to the territory of which, or otherwise under the control of which such item is transferred;

''(iv) any equipment, materials, or software or related technology that significantly contributes to the design or manufacture of a nuclear weapon or other nuclear explosive device, with the intention that it will be used for such purpose, except where—

''(I) the country to the territory of which or under the control of which such item is transferred is a Nuclear Weapon State Party to the Non-Proliferation Treaty; and

''(II) the resulting transfer or receipt (including internal to a country) is not contrary to the obligations under the Non-Proliferation Treaty of a Non-Proliferation Treaty State Party from which, to the territory of which, or otherwise under the control of which such item is transferred;

''(v) any equipment, materials, or software or related technology that significantly contributes to the delivery of a nuclear weapon or other nuclear explosive device, with the intention that it will be used for such purpose, except where—

''(I) such item is transported to or from the territory of, or otherwise under the control of, a Non-Proliferation Treaty State Party; and

''(II) such item is intended for the delivery system of a nuclear weapon or other nuclear explosive device of a Nuclear Weapon State Party to the Non-Proliferation Treaty; or

''(vi) any equipment, materials, or software or related technology that significantly contributes to the design, manufacture, or delivery of a biological or chemical weapon, with the intention that it will be used for such purpose;

''(C) transports another person on board a ship knowing that the person has committed an act that constitutes an offense under section 2280 or subparagraph (A), (B), (D), or (E) of this section or an offense set forth in an applicable treaty, as specified in section 2280(d)(1), and intending to assist that person to evade criminal prosecution;

''(D) injures or kills any person in connection with the commission or the attempted commission of any of the offenses set forth in subparagraphs (A) through (C), or subsection (a)(2), to the extent that the subsection (a)(2) offense pertains to subparagraph (A); or

''(E) attempts to do any act prohibited under subparagraph (A), (B) or (D), or conspires to do any act prohibited by subparagraphs (A) through (E) or subsection (a)(2),

shall be fined under this title, imprisoned not more than 20 years, or both; and if the death of any person results from conduct prohibited by this paragraph, shall be imprisoned for any term of years or for life.

''(2) THREATS.—A person who threatens, with apparent determination and will to carry the threat into execution, to do any act prohibited under paragraph (1)(A) shall be fined under this title, imprisoned not more than 5 years, or both.

''(b) JURISDICTION.—There is jurisdiction over the activity prohibited in subsection (a)—

''(1) in the case of a covered ship, if—

''(A) such activity is committed—

''(i) against or on board a vessel of the United States or a vessel subject to the jurisdiction of the United States (as defined in section 70502 of title 46) at the time the prohibited activity is committed;

''(ii) in the United States, including the territorial seas; or

''(iii) by a national of the United States, by a United States corporation or legal entity, or by a stateless person whose habitual residence is in the United States;

''(B) during the commission of such activity, a national of the United States is seized, threatened, injured, or killed; or

''(C) the offender is later found in the United States after such activity is committed;

''(2) in the case of a ship navigating or scheduled to navigate solely within the territorial sea or internal waters of a country other than the United States, if the offender is later found in the United States after such activity is committed; or

''(3) in the case of any vessel, if such activity is committed in an attempt to compel the United States to do or abstain from doing any act.

''(c) EXCEPTIONS.—This section shall not apply to—

''(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

''(2) activities undertaken by military forces of a state in the exercise of their official duties.

''(d)(1) CIVIL FORFEITURE.—Any real or personal property used or intended to be used to commit or to facilitate the commission of a violation of this section, the gross proceeds of such violation, and any real or personal property traceable to such property or proceeds, shall be subject to forfeiture.

''(2) APPLICABLE PROCEDURES.—Seizures and forfeitures under this section shall be governed by the provisions of chapter 46 of title 18, United States Code, relating to civil forfeitures, except that such duties as are imposed upon the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents, and other persons as may be designated for that purpose by the Secretary of Homeland Security, the Attorney General, or the Secretary of Defense.''.

(b) CONFORMING AMENDMENT.—The table of sections at the beginning of chapter 111 of title 18, United States Code, is amended by adding after the item relating to section 2280 the following new item:

''2280a. Violence against maritime navigation and maritime transport involving weapons of mass destruction.''.

SEC. 803. AMENDMENTS TO SECTION 2281 OF TITLE 18, UNITED STATES CODE.

Section 2281 of title 18, United States Code, is amended—

(1) in subsection (c), by striking ''section 2(c)'' and inserting ''section 13(c)'';

(2) in subsection (d), by striking the definitions of ''national of the United States,'' ''territorial sea of the United States,'' and ''United States''; and

(3) by inserting after subsection (d) the following:

''(e) EXCEPTIONS.—This section does not apply to—

''(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

''(2) activities undertaken by military forces of a state in the exercise of their official duties.''.

SEC. 804. NEW SECTION 2281A OF TITLE 18, UNITED STATES CODE.

(a) IN GENERAL.—Chapter 111 of title 18, United States Code, is amended by adding after section 2281 the following new section:

''§ 2281a. Additional offenses against maritime fixed platforms

''(a) OFFENSES.—

''(1) IN GENERAL.—A person who unlawfully and intentionally—

''(A) when the purpose of the act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act—

''(i) uses against or on a fixed platform or discharges from a fixed platform any explosive or radioactive material, biological, chemical, or nuclear weapon in a manner that causes or is likely to cause death or serious injury or damage; or

''(ii) discharges from a fixed platform oil, liquefied natural gas, or another hazardous or noxious substance that is not covered by clause (i), in such quantity or concentration that causes or is likely to cause death or serious injury or damage;

''(B) injures or kills any person in connection with the commission or the attempted commission of any of the offenses set forth in subparagraph (A); or

''(C) attempts or conspires to do anything prohibited under subparagraph (A) or (B),

shall be fined under this title, imprisoned not more than 20 years, or both; and if death results to any person from conduct prohibited by this paragraph, shall be imprisoned for any term of years or for life.

''(2) THREAT TO SAFETY.—A person who threatens, with apparent determination and will to carry the threat into execution, to do any act prohibited under paragraph (1)(A), shall be fined under this title, imprisoned not more than 5 years, or both.

''(b) JURISDICTION.—There is jurisdiction over the activity prohibited in subsection (a) if—

''(1) such activity is committed against or on board a fixed platform—

''(A) that is located on the continental shelf of the United States;

''(B) that is located on the continental shelf of another country, by a national of the United States or by a stateless person whose habitual residence is in the United States; or

''(C) in an attempt to compel the United States to do or abstain from doing any act;

''(2) during the commission of such activity against or on board a fixed platform located on a continental shelf, a national of the United States is seized, threatened, injured, or killed; or

''(3) such activity is committed against or on board a fixed platform located outside the United States and beyond the continental shelf of the United States and the offender is later found in the United States.

''(c) EXCEPTIONS.—This section does not apply to—

''(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

''(2) activities undertaken by military forces of a state in the exercise of their official duties.

''(d) DEFINITIONS.—In this section—

''(1) 'continental shelf' means the sea-bed and subsoil of the submarine areas that extend beyond a country's territorial sea to the limits provided by customary international law as reflected in Article 76 of the 1982 Convention on the Law of the Sea; and

''(2) 'fixed platform' means an artificial island, installation, or structure permanently attached to the sea-bed for the purpose of exploration or exploitation of resources or for other economic purposes.''.

(b) CONFORMING AMENDMENT.—The table of sections at the beginning of chapter 111 of title 18, United States Code, is amended by adding after the item relating to section 2281 the following new item:

''2281a. Additional offenses against maritime fixed platforms.''.

SEC. 805. ANCILLARY MEASURE.

Section 2332b(g)(5)(B) of title 18, United States Code, is amended by inserting ''2280a (relating to maritime safety),'' before ''2281'', and by striking ''2281'' and inserting ''2281 through 2281a''.

Subtitle B—Prevention of Nuclear Terrorism

SEC. 811. NEW SECTION 2332I OF TITLE 18, UNITED STATES CODE.

(a) IN GENERAL.—Chapter 113B of title 18, United States Code, is amended by adding after section 2332h the following:

''§ 2332i. Acts of nuclear terrorism

''(a) OFFENSES.—

''(1) IN GENERAL.—Whoever knowingly and unlawfully—

''(A) possesses radioactive material or makes or possesses a device—

''(i) with the intent to cause death or serious bodily injury; or

''(ii) with the intent to cause substantial damage to property or the environment; or

''(B) uses in any way radioactive material or a device, or uses or damages or interferes with the operation of a nuclear facility in a manner that causes the release of or increases the risk of the release of radioactive material, or causes radioactive contamination or exposure to radiation—

''(i) with the intent to cause death or serious bodily injury or with the knowledge that such act is likely to cause death or serious bodily injury;

''(ii) with the intent to cause substantial damage to property or the environment or with the knowledge that such act is likely to cause substantial damage to property or the environment; or

''(iii) with the intent to compel a person, an international organization or a country to do or refrain from doing an act,

shall be punished as prescribed in subsection (c).

''(2) THREATS.—Whoever, under circumstances in which the threat may reasonably be believed, threatens to commit an offense under paragraph (1) shall be punished as prescribed in subsection (c). Whoever demands possession of or access to radioactive material, a device or a nuclear facility by threat or by use of force shall be punished as prescribed in subsection (c).

''(3) ATTEMPTS AND CONSPIRACIES.—Whoever attempts to commit an offense under paragraph (1) or conspires to commit an offense under paragraph (1) or (2) shall be punished as prescribed in subsection (c).

''(b) JURISDICTION.—Conduct prohibited by subsection (a) is within the jurisdiction of the United States if—

''(1) the prohibited conduct takes place in the United States or the special aircraft jurisdiction of the United States;

''(2) the prohibited conduct takes place outside of the United States and—

''(A) is committed by a national of the United States, a United States corporation or legal entity or a stateless person whose habitual residence is in the United States;

''(B) is committed on board a vessel of the United States or a vessel subject to the jurisdiction of the United States (as defined in section 70502 of title 46) or on board an aircraft that is registered under United States law, at the time the offense is committed; or

''(C) is committed in an attempt to compel the United States to do or abstain from doing any act, or constitutes a threat directed at the United States;

''(3) the prohibited conduct takes place outside of the United States and a victim or an intended victim is a national of the United States or a United States corporation or legal entity, or the offense is committed against any state or government facility of the United States; or

''(4) a perpetrator of the prohibited conduct is found in the United States.

''(c) PENALTIES.—Whoever violates this section shall be fined not more than $2,000,000 and shall be imprisoned for any term of years or for life.

''(d) NONAPPLICABILITY.—This section does not apply to—

''(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

''(2) activities undertaken by military forces of a state in the exercise of their official duties.

''(e) DEFINITIONS.—As used in this section, the term—

''(1) 'armed conflict' has the meaning given that term in section 2332f(e)(11) of this title;

''(2) 'device' means:

''(A) any nuclear explosive device; or

''(B) any radioactive material dispersal or radiation-emitting device that may, owing to its radiological properties, cause death, serious bodily injury or substantial damage to property or the environment;

''(3) 'international organization' has the meaning given that term in section 831(f)(3) of this title;

''(4) 'military forces of a state' means the armed forces of a country that are organized, trained and equipped under its internal law for the primary purpose of national defense or security and persons acting in support of those armed forces who are under their formal command, control and responsibility;

''(5) 'national of the United States' has the meaning given that term in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22));

''(6) 'nuclear facility' means:

''(A) any nuclear reactor, including reactors on vessels, vehicles, aircraft or space objects for use as an energy source in order to propel such vessels, vehicles, aircraft or space objects or for any other purpose;

''(B) any plant or conveyance being used for the production, storage, processing or transport of radioactive material; or

''(C) a facility (including associated buildings and equipment) in which nuclear material is produced, processed, used, handled, stored or disposed of, if damage to or interference with such facility could lead to the release of significant amounts of radiation or radioactive material;

''(7) 'nuclear material' has the meaning given that term in section 831(f)(1) of this title;

''(8) 'radioactive material' means nuclear material and other radioactive substances that contain nuclides that undergo spontaneous disintegration (a process accompanied by emission of one or more types of ionizing radiation, such as alpha-, beta-, neutron particles and gamma rays) and that may, owing to their radiological or fissile properties, cause death, serious bodily injury or substantial damage to property or to the environment;

''(9) 'serious bodily injury' has the meaning given that term in section 831(f)(4) of this title;

''(10) 'state' has the same meaning as that term has under international law, and includes all political subdivisions thereof;

''(11) 'state or government facility' has the meaning given that term in section 2332f(e)(3) of this title;

''(12) 'United States corporation or legal entity' means any corporation or other entity organized under the laws of the United States or any State, Commonwealth, territory, possession or district of the United States;

''(13) 'vessel' has the meaning given that term in section 1502(19) of title 33; and

''(14) 'vessel of the United States' has the meaning given that term in section 70502 of title 46.''.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 113B of title 18, United States Code, is amended by inserting after the item relating to section 2332h the following:

''2332i. Acts of nuclear terrorism.''.

(c) DISCLAIMER.—Nothing contained in this section is intended to affect the applicability of any other Federal or State law that might pertain to the underlying conduct.

(d) INCLUSION IN DEFINITION OF FEDERAL CRIMES OF TERRORISM.—Section 2332b(g)(5)(B) of title 18, United States Code, is amended by inserting ''2332i (relating to acts of nuclear terrorism),'' before ''2339 (relating to harboring terrorists)''.

SEC. 812. AMENDMENT TO SECTION 831 OF TITLE 18, UNITED STATES CODE.

Section 831 of title 18, United States Code, is amended—

(a) in subsection (a)—

(1) by redesignating paragraphs (3) through (8) as paragraphs (4) through (9);

(2) by inserting after paragraph (2) the following:

''(3) without lawful authority, intentionally carries, sends or moves nuclear material into or out of a country;'';

(3) in paragraph (8), as redesignated, by striking ''an offense under paragraph (1), (2), (3), or (4)'' and inserting ''any act prohibited under paragraphs (1) through (5)''; and

(4) in paragraph (9), as redesignated, by striking ''an offense under paragraph (1), (2), (3), or (4)'' and inserting ''any act prohibited under paragraphs (1) through (7)'';

(b) in subsection (b)—

(1) in paragraph (1), by striking ''(7)'' and inserting ''(8)''; and

(2) in paragraph (2), by striking ''(8)'' and inserting ''(9)'';

(c) in subsection (c)—

(1) in subparagraph (2)(A), by adding after ''United States'' the following: ''or a stateless person whose habitual residence is in the United States'';

(2) by striking paragraph (5);

(3) in paragraph (4), by striking ''or'' at the end; and

(4) by inserting after paragraph (4), the following:

''(5) the offense is committed on board a vessel of the United States or a vessel subject to the jurisdiction of the United States (as defined in section 70502 of title 46) or on board an aircraft that is registered under United States law, at the time the offense is committed;

''(6) the offense is committed outside the United States and against any state or government facility of the United States; or

''(7) the offense is committed in an attempt to compel the United States to do or abstain from doing any act, or constitutes a threat directed at the United States.'';

(d) by redesignating subsections (d) through (f) as (e) through (g), respectively;

(e) by inserting after subsection (c) the following:

''(d) NONAPPLICABILITY.—This section does not apply to—

''(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

''(2) activities undertaken by military forces of a state in the exercise of their official duties.''; and

(f) in subsection (g), as redesignated—

(1) in paragraph (6), by striking ''and'' at the end;

(2) in paragraph (7), by striking the period at the end and inserting a semicolon; and

(3) by inserting after paragraph (7), the following:

''(8) the term 'armed conflict' has the meaning given that term in section 2332f(e)(11) of this title;

''(9) the term 'military forces of a state' means the armed forces of a country that are organized, trained and equipped under its internal law for the primary purpose of national defense or security and persons acting in support of those armed forces who are under their formal command, control and responsibility;

''(10) the term 'state' has the same meaning as that term has under international law, and includes all political subdivisions thereof;

''(11) the term 'state or government facility' has the meaning given that term in section 2332f(e)(3) of this title; and

''(12) the term 'vessel of the United States' has the meaning given that term in section 70502 of title 46.''.

SA 1450. Mr. MCCONNELL proposed an amendment to amendment SA 1449 proposed by Mr. MCCONNELL (for himself and Mr. BURR) to the bill H.R. 2048, to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes; as follows:

Strike Sec. 110(a) and insert the following:

(a) IN GENERAL.—The amendments made by sections 101 through 103 shall take effect on the date that is 12 months after the date of the enactment of this Act.

SA 1451. Mr. MCCONNELL proposed an amendment to amendment SA 1450 proposed by Mr. MCCONNELL to the amendment SA 1449 proposed by Mr. MCCONNELL (for himself and Mr. BURR) to the bill H.R. 2048, to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes; as follows:

At the end, add the following:

(b) NONEFFECT OF CERTAIN PROVISIONS.—Section 401 of this Act, relating to appointment of amicus curiae, shall have no force or effect.

SEC. 110A. APPOINTMENT OF AMICUS CURIAE.

Section 103 (50 U.S.C. 1803) is amended by adding at the end the following new subsections:

''(i) AMICUS CURIAE.—

''(1) AUTHORIZATION.—A court established under subsection (a) or (b) is authorized, consistent with the requirement of subsection (c) and any other statutory requirement that the court act expeditiously or within a stated time—

''(A) to appoint amicus curiae to—

''(i) assist the court in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law; or

''(ii) provide technical expertise in any instance the court considers appropriate; or

''(B) upon motion, to permit an individual or organization leave to file an amicus curiae brief.

''(2) DESIGNATION.—The courts established by subsection (a) and (b) shall each designate 1 or more individuals who may be appointed to serve as amicus curiae and who are determined to be eligible for access to classified national security information necessary to participate in matters before such courts (if such access is necessary for participation in the matters for which they may be appointed). In appointing an amicus curiae pursuant to paragraph (1), the court may choose from among those so designated.

''(3) EXPERTISE.—An individual appointed as an amicus curiae under paragraph (1) may be an individual who possesses expertise on privacy and civil liberties, intelligence collection, communications technology, or any other area that may lend legal or technical expertise to the court.

''(4) DUTIES.—An amicus curiae appointed under paragraph (1) to assist with the consideration of a covered matter shall carry out the duties assigned by the appointing court. That court may authorize the amicus curiae to review any application, certification, petition, motion, or other submission that the court determines is relevant to the duties assigned by the court.

''(5) NOTIFICATION.—A court established under subsection (a) or (b) shall notify the Attorney General of each exercise of the authority to appoint an amicus curiae under paragraph (1).

''(6) ASSISTANCE.—A court established under subsection (a) or (b) may request and receive (including on a non-reimbursable basis) the assistance of the executive branch in the implementation of this subsection.

''(7) ADMINISTRATION.—A court established under subsection (a) or (b) may provide for the designation, appointment, removal, training, or other support of an amicus curiae appointed under paragraph (1) in a manner that is not inconsistent with this subsection.

''(j) REVIEW OF FISA COURT DECISIONS.—Following issuance of an order under this Act, a court established under subsection (a) shall certify for review to the court established under subsection (b) any question of law that may affect resolution of the matter in controversy that the court determines warrants such review because of a need for uniformity or because consideration by the court established under subsection (b) would serve the interests of justice. Upon certification of a question of law under this subsection, the court established under subsection (b) may give binding instructions or require the entire record to be sent up for decision of the entire matter in controversy.

''(k) REVIEW OF FISA COURT OF REVIEW DECISIONS.—

''(1) CERTIFICATION.—For purposes of section 1254(2) of title 28, United States Code, the court of review established under subsection (b) shall be considered to be a court of appeals.

''(2) AMICUS CURIAE BRIEFING.—Upon certification of an application under paragraph (1), the Supreme Court of the United States may appoint an amicus curiae designated under subsection (i)(3), or any other person, to provide briefing or other assistance.''.

SA 1452. Mr. MCCONNELL (for himself and Mr. BURR) proposed an amendment to the bill H.R. 2048, to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes; as follows:

Strike all after the first word and insert the following:

1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015'' or the ''USA FREEDOM Act of 2015''.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

1. Short title; table of contents.
2. Amendments to the Foreign Intelligence Surveillance Act of 1978.

TITLE I—FISA BUSINESS RECORDS REFORMS

101. Additional requirements for call detail records.
102. Emergency authority.
103. Prohibition on bulk collection of tangible things.
104. Judicial review.
105. Liability protection.
106. Compensation for assistance.
107. Notice to the Attorney General on changes in retention of call detail records.
108. Definitions.
109. Inspector General reports on business records orders.
110. Effective date.
111. Rule of construction.

TITLE II—FISA PEN REGISTER AND TRAP AND TRACE DEVICE REFORM

201. Prohibition on bulk collection.
202. Privacy procedures.

TITLE III—FISA ACQUISITIONS TARGETING PERSONS OUTSIDE THE UNITED STATES REFORMS

301. Limits on use of unlawfully obtained information.

TITLE IV—FOREIGN INTELLIGENCE SURVEILLANCE COURT REFORMS

401. Appointment of amicus curiae.

TITLE V—NATIONAL SECURITY LETTER REFORM

501. Prohibition on bulk collection.
502. Limitations on disclosure of national security letters.
503. Judicial review.

TITLE VI—FISA TRANSPARENCY AND REPORTING REQUIREMENTS

601. Additional reporting on orders requiring production of business records; business records compliance reports to Congress.
602. Annual reports by the Government.
603. Public reporting by persons subject to FISA orders.
604. Reporting requirements for decisions, orders, and opinions of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review.
605. Submission of reports under FISA.

TITLE VII—ENHANCED NATIONAL SECURITY PROVISIONS

701. Emergencies involving non-United States persons.
702. Preservation of treatment of non-United States persons traveling outside the United States as agents of foreign powers.
703. Improvement to investigations of international proliferation of weapons of mass destruction.
704. Increase in penalties for material support of foreign terrorist organizations.
705. Sunsets.

TITLE VIII—SAFETY OF MARITIME NAVIGATION AND NUCLEAR TERRORISM CONVENTIONS IMPLEMENTATION

Subtitle A—Safety of Maritime Navigation

801. Amendment to section 2280 of title 18, United States Code.
802. New section 2280a of title 18, United States Code.
803. Amendments to section 2281 of title 18, United States Code.
804. New section 2281a of title 18, United States Code.
805. Ancillary measure.

Subtitle B—Prevention of Nuclear Terrorism

811. New section 2332i of title 18, United States Code.
812. Amendment to section 831 of title 18, United States Code.

SEC. 2. AMENDMENTS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

Except as otherwise expressly provided, whenever in this Act an amendment or repeal is expressed in terms of an amendment to, or a repeal of, a section or other provision, the reference shall be considered to be made to a section or other provision of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

TITLE I—FISA BUSINESS RECORDS REFORMS

SEC. 101. ADDITIONAL REQUIREMENTS FOR CALL DETAIL RECORDS.

(a) APPLICATION.—Section 501(b)(2) (50 U.S.C. 1861(b)(2)) is amended—

(1) in subparagraph (A)—

(A) in the matter preceding clause (i), by striking ''a statement'' and inserting ''in the case of an application other than an application described in subparagraph (C) (including an application for the production of call detail records other than in the manner described in subparagraph (C)), a statement''; and

(B) in clause (iii), by striking ''; and'' and inserting a semicolon;

(2) by redesignating subparagraphs (A) and (B) as subparagraphs (B) and (D), respectively; and

(3) by inserting after subparagraph (B) (as so redesignated) the following new subparagraph:

''(C) in the case of an application for the production on an ongoing basis of call detail records created before, on, or after the date of the application relating to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to protect against international terrorism, a statement of facts showing that—

''(i) there are reasonable grounds to believe that the call detail records sought to be produced based on the specific selection term required under subparagraph (A) are relevant to such investigation; and

''(ii) there is a reasonable, articulable suspicion that such specific selection term is associated with a foreign power engaged in international terrorism or activities in preparation therefor, or an agent of a foreign power engaged in international terrorism or activities in preparation therefor; and''.

(b) ORDER.—Section 501(c)(2) (50 U.S.C. 1861(c)(2)) is amended—

(1) in subparagraph (D), by striking ''; and'' and inserting a semicolon;

(2) in subparagraph (E), by striking the period and inserting ''; and''; and

(3) by adding at the end the following new subparagraph:

''(F) in the case of an application described in subsection (b)(2)(C), shall—

''(i) authorize the production on a daily basis of call detail records for a period not to exceed 180 days;

''(ii) provide that an order for such production may be extended upon application under subsection (b) and the judicial finding under paragraph (1) of this subsection;

''(iii) provide that the Government may require the prompt production of a first set of call detail records using the specific selection term that satisfies the standard required under subsection (b)(2)(C)(ii);

''(iv) provide that the Government may require the prompt production of a second set of call detail records using session-identifying information or a telephone calling card number identified by the specific selection term used to produce call detail records under clause (iii);

''(v) provide that, when produced, such records be in a form that will be useful to the Government;

''(vi) direct each person the Government directs to produce call detail records under the order to furnish the Government forthwith all information, facilities, or technical assistance necessary to accomplish the production in such a manner as will protect the secrecy of the production and produce a minimum of interference with the services that such person is providing to each subject of the production; and

''(vii) direct the Government to—

''(I) adopt minimization procedures that require the prompt destruction of all call detail records produced under the order that the Government determines are not foreign intelligence information; and

''(II) destroy all call detail records produced under the order as prescribed by such procedures.''.

SEC. 102. EMERGENCY AUTHORITY.

(a) AUTHORITY.—Section 501 (50 U.S.C. 1861) is amended by adding at the end the following new subsection:

''(i) EMERGENCY AUTHORITY FOR PRODUCTION OF TANGIBLE THINGS.—

''(1) Notwithstanding any other provision of this section, the Attorney General may require the emergency production of tangible things if the Attorney General—

''(A) reasonably determines that an emergency situation requires the production of tangible things before an order authorizing such production can with due diligence be obtained;

''(B) reasonably determines that the factual basis for the issuance of an order under this section to approve such production of tangible things exists;

''(C) informs, either personally or through a designee, a judge having jurisdiction under this section at the time the Attorney General requires the emergency production of tangible things that the decision has been made to employ the authority under this subsection; and

''(D) makes an application in accordance with this section to a judge having jurisdiction under this section as soon as practicable, but not later than 7 days after the Attorney General requires the emergency production of tangible things under this subsection.

''(2) If the Attorney General requires the emergency production of tangible things under paragraph (1), the Attorney General shall require that the minimization procedures required by this section for the issuance of a judicial order be followed.

''(3) In the absence of a judicial order approving the production of tangible things under this subsection, the production shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time the Attorney General begins requiring the emergency production of such tangible things, whichever is earliest.

''(4) A denial of the application made under this subsection may be reviewed as provided in section 103.

''(5) If such application for approval is denied, or in any other case where the production of tangible things is terminated and no order is issued approving the production, no information obtained or evidence derived from such production shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof, and no information concerning any United States person acquired from such production shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

''(6) The Attorney General shall assess compliance with the requirements of paragraph (5).''.

(b) CONFORMING AMENDMENT.—Section 501(d) (50 U.S.C. 1861(d)) is amended—

(1) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking ''pursuant to an order'' and inserting ''pursuant to an order issued or an emergency production required'';

(B) in subparagraph (A), by striking ''such order'' and inserting ''such order or such emergency production''; and

(C) in subparagraph (B), by striking ''the order'' and inserting ''the order or the emergency production''; and

(2) in paragraph (2)—

(A) in subparagraph (A), by striking ''an order'' and inserting ''an order or emergency production''; and

(B) in subparagraph (B), by striking ''an order'' and inserting ''an order or emergency production''.

SEC. 103. PROHIBITION ON BULK COLLECTION OF TANGIBLE THINGS.

(a) APPLICATION.—Section 501(b)(2) (50 U.S.C. 1861(b)(2)), as amended by section 101(a) of this Act, is further amended by inserting before subparagraph (B), as redesignated by such section 101(a) of this Act, the following new subparagraph:

''(A) a specific selection term to be used as the basis for the production of the tangible things sought;''.

(b) ORDER.—Section 501(c) (50 U.S.C. 1861(c)) is amended—

(1) in paragraph (2)(A), by striking the semicolon and inserting '', including each specific selection term to be used as the basis for the production;''; and

(2) by adding at the end the following new paragraph:

''(3) No order issued under this subsection may authorize the collection of tangible things without the use of a specific selection term that meets the requirements of subsection (b)(2).''.

SEC. 104. JUDICIAL REVIEW.

(a) MINIMIZATION PROCEDURES.—

(1) JUDICIAL REVIEW.—Section 501(c)(1) (50 U.S.C. 1861(c)(1)) is amended by inserting after ''subsections (a) and (b)'' the following: ''and that the minimization procedures submitted in accordance with subsection (b)(2)(D) meet the definition of minimization procedures under subsection (g)''.

(2) RULE OF CONSTRUCTION.—Section 501(g) (50 U.S.C. 1861(g)) is amended by adding at the end the following new paragraph:

''(3) RULE OF CONSTRUCTION.—Nothing in this subsection shall limit the authority of the court established under section 103(a) to impose additional, particularized minimization procedures with regard to the production, retention, or dissemination of nonpublicly available information concerning unconsenting United States persons, including additional, particularized procedures related to the destruction of information within a reasonable time period.''.

(3) TECHNICAL AND CONFORMING AMENDMENT.—Section 501(g)(1) (50 U.S.C. 1861(g)(1)) is amended—

(A) by striking ''Not later than 180 days after the date of the enactment of the USA PATRIOT Improvement and Reauthorization Act of 2005, the'' and inserting ''The''; and

(B) by inserting after ''adopt'' the following: '', and update as appropriate,''.

(b) ORDERS.—Section 501(f)(2) (50 U.S.C. 1861(f)(2)) is amended—

(1) in subparagraph (A)(i)—

(A) by striking ''that order'' and inserting ''the production order or any nondisclosure order imposed in connection with the production order''; and

(B) by striking the second sentence; and

(2) in subparagraph (C)—

(A) by striking clause (ii); and

(B) by redesignating clause (iii) as clause (ii).

SEC. 105. LIABILITY PROTECTION.

Section 501(e) (50 U.S.C. 1861(e)) is amended to read as follows:

''(e)(1) No cause of action shall lie in any court against a person who—

''(A) produces tangible things or provides information, facilities, or technical assistance in accordance with an order issued or an emergency production required under this section; or

''(B) otherwise provides technical assistance to the Government under this section or to implement the amendments made to this section by the USA FREEDOM Act of 2015.

''(2) A production or provision of information, facilities, or technical assistance described in paragraph (1) shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.''.

SEC. 106. COMPENSATION FOR ASSISTANCE.

Section 501 (50 U.S.C. 1861), as amended by section 102 of this Act, is further amended by adding at the end the following new subsection:

''(j) COMPENSATION.—The Government shall compensate a person for reasonable expenses incurred for—

''(1) producing tangible things or providing information, facilities, or assistance in accordance with an order issued with respect to an application described in subsection (b)(2)(C) or an emergency production under subsection (i) that, to comply with subsection (i)(1)(D), requires an application described in subsection (b)(2)(C); or

''(2) otherwise providing technical assistance to the Government under this section or to implement the amendments made to this section by the USA FREEDOM Act of 2015.''.

SEC. 107. NOTICE TO THE ATTORNEY GENERAL ON CHANGES IN RETENTION OF CALL DETAIL RECORDS.

Section 501 (50 U.S.C. 1861), as amended by section 106 of this Act, is amended by adding at the end the following new subsection:

''(k) PROSPECTIVE CHANGES TO EXISTING PRACTICES RELATED TO CALL DETAIL RECORDS.—

''(1) IN GENERAL.—Consistent with subsection (c)(2)(F), an electronic communication service provider that has been issued an order to produce call detail records pursuant to an order under subsection (c) shall notify the Attorney General if that service provider intends to retain its call detail records for a period less than 18 months.

''(2) TIMING OF NOTICE.—A notification under paragraph (1) shall be made not less than 180 days prior to the date such electronic communications service provider intends to implement a policy to retain such records for a period less than 18 months.''.

SEC. 108. DEFINITIONS.

Section 501 (50 U.S.C. 1861), as amended by section 107 of this Act, is further amended by adding at the end the following new subsection:

''(l) DEFINITIONS.—In this section:

''(1) IN GENERAL.—The terms 'foreign power', 'agent of a foreign power', 'international terrorism', 'foreign intelligence information', 'Attorney General', 'United States person', 'United States', 'person', and 'State' have the meanings provided those terms in section 101.

''(2) ADDRESS.—The term 'address' means a physical address or electronic address, such as an electronic mail address or temporarily assigned network address (including an Internet protocol address).

''(3) CALL DETAIL RECORD.—The term 'call detail record'—

''(A) means session-identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity number, or an International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call; and

''(B) does not include—

''(i) the contents (as defined in section 2510(8) of title 18, United States Code) of any communication;

''(ii) the name, address, or financial information of a subscriber or customer; or

''(iii) cell site location or global positioning system information.

''(4) SPECIFIC SELECTION TERM.—

''(A) TANGIBLE THINGS.—

''(i) IN GENERAL.—Except as provided in subparagraph (B), a 'specific selection term'—

''(I) is a term that specifically identifies a person, account, address, or personal device, or any other specific identifier; and

''(II) is used to limit, to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things.

''(ii) LIMITATION.—A specific selection term under clause (i) does not include an identifier that does not limit, to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things, such as an identifier that—

''(I) identifies an electronic communication service provider (as that term is defined in section 701) or a provider of remote computing service (as that term is defined in section 2711 of title 18, United States Code), when not used as part of a specific identifier as described in clause (i), unless the provider is itself a subject of an authorized investigation for which the specific selection term is used as the basis for the production; or

''(II) identifies a broad geographic region, including the United States, a city, a county, a State, a zip code, or an area code, when not used as part of a specific identifier as described in clause (i).

''(iii) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to preclude the use of multiple terms or identifiers to meet the requirements of clause (i).

''(B) CALL DETAIL RECORD APPLICATIONS.—For purposes of an application submitted under subsection (b)(2)(C), the term 'specific selection term' means a term that specifically identifies an individual, account, or personal device.''.

SEC. 109. INSPECTOR GENERAL REPORTS ON BUSINESS RECORDS ORDERS.

Section 106A of the USA PATRIOT Improvement and Reauthorization Act of 2005 (Public Law 109–177; 120 Stat. 200) is amended—

(1) in subsection (b)—

(A) in paragraph (1), by inserting ''and calendar years 2012 through 2014'' after ''2006'';

(B) by striking paragraphs (2) and (3);

(C) by redesignating paragraphs (4) and (5) as paragraphs (2) and (3), respectively; and

(D) in paragraph (3) (as so redesignated)—

(i) by striking subparagraph (C) and inserting the following new subparagraph:

''(C) with respect to calendar years 2012 through 2014, an examination of the minimization procedures used in relation to orders under section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861) and whether the minimization procedures adequately protect the constitutional rights of United States persons;''; and

(ii) in subparagraph (D), by striking ''(as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)))'';

(2) in subsection (c), by adding at the end the following new paragraph:

''(3) CALENDAR YEARS 2012 THROUGH 2014.—Not later than 1 year after the date of enactment of the USA FREEDOM Act of 2015, the Inspector General of the Department of Justice shall submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives a report containing the results of the audit conducted under subsection (a) for calendar years 2012 through 2014.'';

(3) by redesignating subsections (d) and (e) as subsections (e) and (f), respectively;

(4) by inserting after subsection (c) the following new subsection:

''(d) INTELLIGENCE ASSESSMENT.—

''(1) IN GENERAL.—For the period beginning on January 1, 2012, and ending on December 31, 2014, the Inspector General of the Intelligence Community shall assess—

''(A) the importance of the information acquired under title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) to the activities of the intelligence community;

''(B) the manner in which that information was collected, retained, analyzed, and disseminated by the intelligence community;

''(C) the minimization procedures used by elements of the intelligence community under such title and whether the minimization procedures adequately protect the constitutional rights of United States persons; and

''(D) any minimization procedures proposed by an element of the intelligence community under such title that were modified or denied by the court established under section 103(a) of such Act (50 U.S.C. 1803(a)).

''(2) SUBMISSION DATE FOR ASSESSMENT.—Not later than 180 days after the date on which the Inspector General of the Department of Justice submits the report required under subsection (c)(3), the Inspector General of the Intelligence Community shall submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives a report containing the results of the assessment for calendar years 2012 through 2014.'';

(5) in subsection (e), as redesignated by paragraph (3)—

(A) in paragraph (1)—

(i) by striking ''a report under subsection (c)(1) or (c)(2)'' and inserting ''any report under subsection (c) or (d)''; and

(ii) by striking ''Inspector General of the Department of Justice'' and inserting ''Inspector General of the Department of Justice, the Inspector General of the Intelligence Community, and any Inspector General of an element of the intelligence community that prepares a report to assist the Inspector General of the Department of Justice or the Inspector General of the Intelligence Community in complying with the requirements of this section''; and

(B) in paragraph (2), by striking ''the reports submitted under subsections (c)(1) and (c)(2)'' and inserting ''any report submitted under subsection (c) or (d)'';

(6) in subsection (f), as redesignated by paragraph (3)—

(A) by striking ''The reports submitted under subsections (c)(1) and (c)(2)'' and inserting ''Each report submitted under subsection (c)''; and

(B) by striking ''subsection (d)(2)'' and inserting ''subsection (e)(2)''; and

(7) by adding at the end the following new subsection:

''(g) DEFINITIONS.—In this section:

''(1) INTELLIGENCE COMMUNITY.—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).

''(2) UNITED STATES PERSON.—The term 'United States person' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).''.

SEC. 110. EFFECTIVE DATE.

(a) IN GENERAL.—The amendments made by sections 101 through 103 shall take effect on the date that is 1 year after the date of the enactment of this Act.

(b) REVIEW AND CERTIFICATION.—The Director of National Intelligence shall—

(1) review the implementation of the transition from the existing procedures for the production of call detail records under title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as in effect prior to the effective date for the amendments made by sections 101 through 103 of this Act, to the new procedures pursuant to the amendments made by sections 101 through 103 of this Act; and

(2) not later than 30 days before the effective date specified in subsection (a), certify to Congress in writing that—

(A) the implementation of the transition described in paragraph (1) is operationally effective to allow the timely retrieval of foreign intelligence information from recipients of an order issued under section 501(c)(2)(F) of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101 of this Act; and

(B) the implementation of the amendments made by section 101 through 103 of this Act—

(i) will not harm the national security of the United States; and

(ii) will ensure the protection of classified information and classified intelligence sources and methods related to such production of call detail records.

(c) RULE OF CONSTRUCTION.—Nothing in this Act shall be construed to alter or eliminate the authority of the Government to obtain an order under title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) as in effect prior to the effective date described in subsection (a) during the period ending on such effective date.

SEC. 111. RULE OF CONSTRUCTION.

Nothing in this Act shall be construed to authorize the production of the contents (as such term is defined in section 2510(8) of title 18, United States Code) of any electronic communication from an electronic communication service provider (as such term is defined in section 701(b)(4) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881(b)(4))) under title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.).

TITLE II—FISA PEN REGISTER AND TRAP AND TRACE DEVICE REFORM

SEC. 201. PROHIBITION ON BULK COLLECTION.

(a) PROHIBITION.—Section 402(c) (50 U.S.C. 1842(c)) is amended—

(1) in paragraph (1), by striking ''; and'' and inserting a semicolon;

(2) in paragraph (2), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following new paragraph:

''(3) a specific selection term to be used as the basis for the use of the pen register or trap and trace device.''.

(b) DEFINITION.—Section 401 (50 U.S.C. 1841) is amended by adding at the end the following new paragraph:

''(4)(A) The term 'specific selection term'—

''(i) is a term that specifically identifies a person, account, address, or personal device, or any other specific identifier; and

''(ii) is used to limit, to the greatest extent reasonably practicable, the scope of information sought, consistent with the purpose for seeking the use of the pen register or trap and trace device.

''(B) A specific selection term under subparagraph (A) does not include an identifier that does not limit, to the greatest extent reasonably practicable, the scope of information sought, consistent with the purpose for seeking the use of the pen register or trap and trace device, such as an identifier that—

''(i) identifies an electronic communication service provider (as that term is defined in section 701) or a provider of remote computing service (as that term is defined in section 2711 of title 18, United States Code), when not used as part of a specific identifier as described in subparagraph (A), unless the provider is itself a subject of an authorized investigation for which the specific selection term is used as the basis for the use; or

''(ii) identifies a broad geographic region, including the United States, a city, a county, a State, a zip code, or an area code, when not used as part of a specific identifier as described in subparagraph (A).

''(C) For purposes of subparagraph (A), the term 'address' means a physical address or electronic address, such as an electronic mail address or temporarily assigned network address (including an Internet protocol address).

''(D) Nothing in this paragraph shall be construed to preclude the use of multiple terms or identifiers to meet the requirements of subparagraph (A).''.

SEC. 202. PRIVACY PROCEDURES.

(a) IN GENERAL.—Section 402 (50 U.S.C. 1842) is amended by adding at the end the following new subsection:

''(h) PRIVACY PROCEDURES.—

''(1) IN GENERAL.—The Attorney General shall ensure that appropriate policies and procedures are in place to safeguard nonpublicly available information concerning United States persons that is collected through the use of a pen register or trap and trace device installed under this section. Such policies and procedures shall, to the maximum extent practicable and consistent with the need to protect national security, include privacy protections that apply to the collection, retention, and use of information concerning United States persons.

''(2) RULE OF CONSTRUCTION.—Nothing in this subsection limits the authority of the court established under section 103(a) or of the Attorney General to impose additional privacy or minimization procedures with regard to the installation or use of a pen register or trap and trace device.''.

(b) EMERGENCY AUTHORITY.—Section 403 (50 U.S.C. 1843) is amended by adding at the end the following new subsection:

''(d) PRIVACY PROCEDURES.—Information collected through the use of a pen register or trap and trace device installed under this section shall be subject to the policies and procedures required under section 402(h).''.

TITLE III—FISA ACQUISITIONS TARGETING PERSONS OUTSIDE THE UNITED STATES REFORMS

SEC. 301. LIMITS ON USE OF UNLAWFULLY OBTAINED INFORMATION.

Section 702(i)(3) (50 U.S.C. 1881a(i)(3)) is amended by adding at the end the following new subparagraph:

''(D) LIMITATION ON USE OF INFORMATION.—

''(i) IN GENERAL.—Except as provided in clause (ii), if the Court orders a correction of a deficiency in a certification or procedures under subparagraph (B), no information obtained or evidence derived pursuant to the part of the certification or procedures that has been identified by the Court as deficient concerning any United States person shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired pursuant to such part of such certification or procedures shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of the United States person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

''(ii) EXCEPTION.—If the Government corrects any deficiency identified by the order of the Court under subparagraph (B), the Court may permit the use or disclosure of information obtained before the date of the correction under such minimization procedures as the Court may approve for purposes of this clause.''.

TITLE IV—FOREIGN INTELLIGENCE SURVEILLANCE COURT REFORMS

SEC. 401. APPOINTMENT OF AMICUS CURIAE.

Section 103 (50 U.S.C. 1803) is amended by adding at the end the following new subsections:

''(i) AMICUS CURIAE.—

''(1) AUTHORIZATION.—A court established under subsection (a) or (b) is authorized, consistent with the requirement of subsection (c) and any other statutory requirement that the court act expeditiously or within a stated time—

''(A) to appoint amicus curiae to—

''(i) assist the court in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law; or

''(ii) provide technical expertise in any instance the court considers appropriate; or

''(B) upon motion, to permit an individual or organization leave to file an amicus curiae brief.

''(2) DESIGNATION.—The courts established by subsection (a) and (b) shall each designate 1 or more individuals who may be appointed to serve as amicus curiae and who are determined to be eligible for access to classified national security information necessary to participate in matters before such courts (if such access is necessary for participation in the matters for which they may be appointed). In appointing an amicus curiae pursuant to paragraph (1), the court may choose from among those so designated.

''(3) EXPERTISE.—An individual appointed as an amicus curiae under paragraph (1) may be an individual who possesses expertise on privacy and civil liberties, intelligence collection, communications technology, or any other area that may lend legal or technical expertise to the court.

''(4) DUTIES.—An amicus curiae appointed under paragraph (1) to assist with the consideration of a covered matter shall carry out the duties assigned by the appointing court. That court may authorize the amicus curiae to review any application, certification, petition, motion, or other submission that the court determines is relevant to the duties assigned by the court.

''(5) NOTIFICATION.—A court established under subsection (a) or (b) shall notify the Attorney General of each exercise of the authority to appoint an amicus curiae under paragraph (1).

''(6) ASSISTANCE.—A court established under subsection (a) or (b) may request and receive (including on a non-reimbursable basis) the assistance of the executive branch in the implementation of this subsection.

''(7) ADMINISTRATION.—A court established under subsection (a) or (b) may provide for the designation, appointment, removal, training, or other support of an amicus curiae appointed under paragraph (1) in a manner that is not inconsistent with this subsection.

''(j) REVIEW OF FISA COURT DECISIONS.—Following issuance of an order under this Act, a court established under subsection (a) shall certify for review to the court established under subsection (b) any question of law that may affect resolution of the matter in controversy that the court determines warrants such review because of a need for uniformity or because consideration by the court established under subsection (b) would serve the interests of justice. Upon certification of a question of law under this subsection, the court established under subsection (b) may give binding instructions or require the entire record to be sent up for decision of the entire matter in controversy.

''(k) REVIEW OF FISA COURT OF REVIEW DECISIONS.—

''(1) CERTIFICATION.—For purposes of section 1254(2) of title 28, United States Code, the court of review established under subsection (b) shall be considered to be a court of appeals.

''(2) AMICUS CURIAE BRIEFING.—Upon certification of an application under paragraph (1), the Supreme Court of the United States

may appoint an amicus curiae designated under subsection (i)(3), or any other person, to provide briefing or other assistance.''.

TITLE V—NATIONAL SECURITY LETTER REFORM

SEC. 501. PROHIBITION ON BULK COLLECTION.

(a) COUNTERINTELLIGENCE ACCESS TO TELEPHONE TOLL AND TRANSACTIONAL RECORDS.—Section 2709(b) of title 18, United States Code, is amended in the matter preceding paragraph (1) by striking ''may'' and inserting ''may, using a term that specifically identifies a person, entity, telephone number, or account as the basis for a request''.

(b) ACCESS TO FINANCIAL RECORDS FOR CERTAIN INTELLIGENCE AND PROTECTIVE PURPOSES.—Section 1114(a)(2) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(2)) is amended by striking the period and inserting ''and a term that specifically identifies a customer, entity, or account to be used as the basis for the production and disclosure of financial records.''.

(c) DISCLOSURES TO FBI OF CERTAIN CONSUMER RECORDS FOR COUNTERINTELLIGENCE PURPOSES.—Section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) is amended—

(1) in subsection (a), by striking ''that information,'' and inserting ''that information that includes a term that specifically identifies a consumer or account to be used as the basis for the production of that information,'';

(2) in subsection (b), by striking ''written request,'' and inserting ''written request that includes a term that specifically identifies a consumer or account to be used as the basis for the production of that information,''; and

(3) in subsection (c), by inserting '', which shall include a term that specifically identifies a consumer or account to be used as the basis for the production of the information,'' after ''issue an order ex parte''.

(d) DISCLOSURES TO GOVERNMENTAL AGENCIES FOR COUNTERTERRORISM PURPOSES OF CONSUMER REPORTS.—Section 627(a) of the Fair Credit Reporting Act (15 U.S.C. 1681v(a)) is amended by striking ''analysis.'' and inserting ''analysis and that includes a term that specifically identifies a consumer or account to be used as the basis for the production of such information.''.

SEC. 502. LIMITATIONS ON DISCLOSURE OF NATIONAL SECURITY LETTERS.

(a) COUNTERINTELLIGENCE ACCESS TO TELEPHONE TOLL AND TRANSACTIONAL RECORDS.—Section 2709 of title 18, United States Code, is amended by striking subsection (c) and inserting the following new subsection:

''(c) PROHIBITION OF CERTAIN DISCLOSURE.—

''(1) PROHIBITION.—

''(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (d) is provided, no wire or electronic communication service provider that receives a request under subsection (b), or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

''(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office, certifies that the absence of a prohibition of disclosure under this subsection may result in—

''(i) a danger to the national security of the United States;

''(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

''(iii) interference with diplomatic relations; or

''(iv) danger to the life or physical safety of any person.

''(2) EXCEPTION.—

''(A) IN GENERAL.—A wire or electronic communication service provider that receives a request under subsection (b), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

''(i) those persons to whom disclosure is necessary in order to comply with the request;

''(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

''(iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

''(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (b) in the same manner as the person to whom the request is issued.

''(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall notify the person of the applicable nondisclosure requirement.

''(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.''.

(b) ACCESS TO FINANCIAL RECORDS FOR CERTAIN INTELLIGENCE AND PROTECTIVE PURPOSES.—Section 1114 of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414) is amended—

(1) in subsection (a)(5), by striking subparagraph (D); and

(2) by inserting after subsection (b) the following new subsection:

''(c) PROHIBITION OF CERTAIN DISCLOSURE.—

''(1) PROHIBITION.—

''(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (d) is provided, no financial institution that receives a request under subsection (a), or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under subsection (a).

''(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office, certifies that the absence of a prohibition of disclosure under this subsection may result in—

''(i) a danger to the national security of the United States;

''(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

''(iii) interference with diplomatic relations; or

''(iv) danger to the life or physical safety of any person.

''(2) EXCEPTION.—

''(A) IN GENERAL.—A financial institution that receives a request under subsection (a), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

''(i) those persons to whom disclosure is necessary in order to comply with the request;

''(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

''(iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

''(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (a) in the same manner as the person to whom the request is issued.

''(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

''(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.''.

(c) IDENTITY OF FINANCIAL INSTITUTIONS AND CREDIT REPORTS.—Section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) is amended by striking subsection (d) and inserting the following new subsection:

''(d) PROHIBITION OF CERTAIN DISCLOSURE.—

''(1) PROHIBITION.—

''(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (e) is provided, no consumer reporting agency that receives a request under subsection (a) or (b) or an order under subsection (c), or officer, employee, or agent thereof, shall disclose or specify in any consumer report, that the Federal Bureau of Investigation has sought or obtained access to information or records under subsection (a), (b), or (c).

''(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office, certifies that the absence of a prohibition of disclosure under this subsection may result in—

''(i) a danger to the national security of the United States;

''(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

''(iii) interference with diplomatic relations; or

''(iv) danger to the life or physical safety of any person.

''(2) EXCEPTION.—

''(A) IN GENERAL.—A consumer reporting agency that receives a request under subsection (a) or (b) or an order under subsection (c), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

''(i) those persons to whom disclosure is necessary in order to comply with the request;

''(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

''(iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

''(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request

under subsection (a) or (b) or an order under subsection (c) is issued in the same manner as the person to whom the request is issued.

''(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

''(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.''.

(d) CONSUMER REPORTS.—Section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v) is amended by striking subsection (c) and inserting the following new subsection:

''(c) PROHIBITION OF CERTAIN DISCLOSURE.—

''(1) PROHIBITION.—

''(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (d) is provided, no consumer reporting agency that receives a request under subsection (a), or officer, employee, or agent thereof, shall disclose or specify in any consumer report, that a government agency described in subsection (a) has sought or obtained access to information or records under subsection (a).

''(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the head of the government agency described in subsection (a), or a designee, certifies that the absence of a prohibition of disclosure under this subsection may result in—

''(i) a danger to the national security of the United States;

''(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

''(iii) interference with diplomatic relations; or

''(iv) danger to the life or physical safety of any person.

''(2) EXCEPTION.—

''(A) IN GENERAL.—A consumer reporting agency that receives a request under subsection (a), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

''(i) those persons to whom disclosure is necessary in order to comply with the request;

''(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

''(iii) other persons as permitted by the head of the government agency described in subsection (a) or a designee.

''(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request under subsection (a) is issued in the same manner as the person to whom the request is issued.

''(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

''(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the head of the government agency described in subsection (a) or a designee, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the head or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.''.

(e) INVESTIGATIONS OF PERSONS WITH ACCESS TO CLASSIFIED INFORMATION.—Section 802 of the National Security Act of 1947 (50 U.S.C. 3162) is amended by striking subsection (b) and inserting the following new subsection:

''(b) PROHIBITION OF CERTAIN DISCLOSURE.—

''(1) PROHIBITION.—

''(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (c) is provided, no governmental or private entity that receives a request under subsection (a), or officer, employee, or agent thereof, shall disclose to any person that an authorized investigative agency described in subsection (a) has sought or obtained access to information under subsection (a).

''(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the head of an authorized investigative agency described in subsection (a), or a designee, certifies that the absence of a prohibition of disclosure under this subsection may result in—

''(i) a danger to the national security of the United States;

''(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

''(iii) interference with diplomatic relations; or

''(iv) danger to the life or physical safety of any person.

''(2) EXCEPTION.—

''(A) IN GENERAL.—A governmental or private entity that receives a request under subsection (a), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

''(i) those persons to whom disclosure is necessary in order to comply with the request;

''(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

''(iii) other persons as permitted by the head of the authorized investigative agency described in subsection (a) or a designee.

''(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (a) in the same manner as the person to whom the request is issued.

''(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

''(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the head of an authorized investigative agency described in subsection (a), or a designee, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the head of the authorized investigative agency or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.''.

(f) TERMINATION PROCEDURES.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Attorney General shall adopt procedures with respect to nondisclosure requirements issued pursuant to section 2709 of title 18, United States Code, section 626 or 627 of the Fair Credit Reporting Act (15 U.S.C. 1681u and 1681v), section 1114 of the Right to Financial Privacy Act (12 U.S.C. 3414), or section 802 of the National Security Act of 1947 (50 U.S.C. 3162), as amended by this Act, to require—

(A) the review at appropriate intervals of such a nondisclosure requirement to assess whether the facts supporting nondisclosure continue to exist;

(B) the termination of such a nondisclosure requirement if the facts no longer support nondisclosure; and

(C) appropriate notice to the recipient of the national security letter, or officer, employee, or agent thereof, subject to the nondisclosure requirement, and the applicable court as appropriate, that the nondisclosure requirement has been terminated.

(2) REPORTING.—Upon adopting the procedures required under paragraph (1), the Attorney General shall submit the procedures to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives.

(g) JUDICIAL REVIEW.—Section 3511 of title 18, United States Code, is amended by striking subsection (b) and inserting the following new subsection:

''(b) NONDISCLOSURE.—

''(1) IN GENERAL.—

''(A) NOTICE.—If a recipient of a request or order for a report, records, or other information under section 2709 of this title, section 626 or 627 of the Fair Credit Reporting Act (15 U.S.C. 1681u and 1681v), section 1114 of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414), or section 802 of the National Security Act of 1947 (50 U.S.C. 3162), wishes to have a court review a nondisclosure requirement imposed in connection with the request or order, the recipient may notify the Government or file a petition for judicial review in any court described in subsection (a).

''(B) APPLICATION.—Not later than 30 days after the date of receipt of a notification under subparagraph (A), the Government shall apply for an order prohibiting the disclosure of the existence or contents of the relevant request or order. An application under this subparagraph may be filed in the district court of the United States for the judicial district in which the recipient of the order is doing business or in the district court of the United States for any judicial district within which the authorized investigation that is the basis for the request is being conducted. The applicable nondisclosure requirement shall remain in effect during the pendency of proceedings relating to the requirement.

''(C) CONSIDERATION.—A district court of the United States that receives a petition under subparagraph (A) or an application under subparagraph (B) should rule expeditiously, and shall, subject to paragraph (3), issue a nondisclosure order that includes conditions appropriate to the circumstances.

''(2) APPLICATION CONTENTS.—An application for a nondisclosure order or extension thereof or a response to a petition filed under paragraph (1) shall include a certification from the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation, or a designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, or in the case of a request by a department, agency, or instrumentality of the Federal Government other than the Department of Justice, the head or deputy head of the department, agency, or instrumentality, containing a statement of specific facts indicating that the absence of a prohibition of disclosure under this subsection may result in—

''(A) a danger to the national security of the United States;

''(B) interference with a criminal, counterterrorism, or counterintelligence investigation;

''(C) interference with diplomatic relations; or

''(D) danger to the life or physical safety of any person.

''(3) STANDARD.—A district court of the United States shall issue a nondisclosure order or extension thereof under this subsection if the court determines that there is reason to believe that disclosure of the information subject to the nondisclosure requirement during the applicable time period may result in—

''(A) a danger to the national security of the United States;

''(B) interference with a criminal, counterterrorism, or counterintelligence investigation;

''(C) interference with diplomatic relations; or

''(D) danger to the life or physical safety of any person.''.

SEC. 503. JUDICIAL REVIEW.

(a) COUNTERINTELLIGENCE ACCESS TO TELEPHONE TOLL AND TRANSACTIONAL RECORDS.—Section 2709 of title 18, United States Code, is amended—

(1) by redesignating subsections (d), (e), and (f) as subsections (e), (f), and (g), respectively; and

(2) by inserting after subsection (c) the following new subsection:

''(d) JUDICIAL REVIEW.—

''(1) IN GENERAL.—A request under subsection (b) or a nondisclosure requirement imposed in connection with such request under subsection (c) shall be subject to judicial review under section 3511.

''(2) NOTICE.—A request under subsection (b) shall include notice of the availability of judicial review described in paragraph (1).''.

(b) ACCESS TO FINANCIAL RECORDS FOR CERTAIN INTELLIGENCE AND PROTECTIVE PURPOSES.—Section 1114 of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414) is amended—

(1) by redesignating subsection (d) as subsection (e); and

(2) by inserting after subsection (c) the following new subsection:

''(d) JUDICIAL REVIEW.—

''(1) IN GENERAL.—A request under subsection (a) or a nondisclosure requirement imposed in connection with such request under subsection (c) shall be subject to judicial review under section 3511 of title 18, United States Code.

''(2) NOTICE.—A request under subsection (a) shall include notice of the availability of judicial review described in paragraph (1).''.

(c) IDENTITY OF FINANCIAL INSTITUTIONS AND CREDIT REPORTS.—Section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) is amended—

(1) by redesignating subsections (e) through (m) as subsections (f) through (n), respectively; and

(2) by inserting after subsection (d) the following new subsection:

''(e) JUDICIAL REVIEW.—

''(1) IN GENERAL.—A request under subsection (a) or (b) or an order under subsection (c) or a non-disclosure requirement imposed in connection with such request under subsection (d) shall be subject to judicial review under section 3511 of title 18, United States Code.

''(2) NOTICE.—A request under subsection (a) or (b) or an order under subsection (c) shall include notice of the availability of judicial review described in paragraph (1).''.

(d) IDENTITY OF FINANCIAL INSTITUTIONS AND CREDIT REPORTS.—Section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v) is amended—

(1) by redesignating subsections (d), (e), and (f) as subsections (e), (f), and (g), respectively; and

(2) by inserting after subsection (c) the following new subsection:

''(d) JUDICIAL REVIEW.—

''(1) IN GENERAL.—A request under subsection (a) or a non-disclosure requirement imposed in connection with such request under subsection (c) shall be subject to judicial review under section 3511 of title 18, United States Code.

''(2) NOTICE.—A request under subsection (a) shall include notice of the availability of judicial review described in paragraph (1).''.

(e) INVESTIGATIONS OF PERSONS WITH ACCESS TO CLASSIFIED INFORMATION.—Section 802 of the National Security Act of 1947 (50 U.S.C. 3162) is amended—

(1) by redesignating subsections (c) through (f) as subsections (d) through (g), respectively; and

(2) by inserting after subsection (b) the following new subsection:

''(c) JUDICIAL REVIEW.—

''(1) IN GENERAL.—A request under subsection (a) or a nondisclosure requirement imposed in connection with such request under subsection (b) shall be subject to judicial review under section 3511 of title 18, United States Code.

''(2) NOTICE.—A request under subsection (a) shall include notice of the availability of judicial review described in paragraph (1).''.

TITLE VI—FISA TRANSPARENCY AND REPORTING REQUIREMENTS

SEC. 601. ADDITIONAL REPORTING ON ORDERS REQUIRING PRODUCTION OF BUSINESS RECORDS; BUSINESS RECORDS COMPLIANCE REPORTS TO CONGRESS.

(a) REPORTS SUBMITTED TO COMMITTEES.—Section 502(b) (50 U.S.C. 1862(b)) is amended—

(1) by redesignating paragraphs (1), (2), and (3) as paragraphs (6), (7), and (8), respectively; and

(2) by inserting before paragraph (6) (as so redesignated) the following new paragraphs:

''(1) a summary of all compliance reviews conducted by the Government for the production of tangible things under section 501;

''(2) the total number of applications described in section 501(b)(2)(B) made for orders approving requests for the production of tangible things;

''(3) the total number of such orders either granted, modified, or denied;

''(4) the total number of applications described in section 501(b)(2)(C) made for orders approving requests for the production of call detail records;

''(5) the total number of such orders either granted, modified, or denied;''.

(b) REPORTING ON CERTAIN TYPES OF PRODUCTION.—Section 502(c)(1) (50 U.S.C. 1862(c)(1)) is amended—

(1) in subparagraph (A), by striking ''and'';

(2) in subparagraph (B), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following new subparagraphs:

''(C) the total number of applications made for orders approving requests for the production of tangible things under section 501 in which the specific selection term does not specifically identify an individual, account, or personal device;

''(D) the total number of orders described in subparagraph (C) either granted, modified, or denied; and

''(E) with respect to orders described in subparagraph (D) that have been granted or modified, whether the court established under section 103 has directed additional, particularized minimization procedures beyond those adopted pursuant to section 501(g).''.

SEC. 602. ANNUAL REPORTS BY THE GOVERNMENT.

(a) IN GENERAL.—Title VI (50 U.S.C. 1871 et seq.), as amended by section 402 of this Act, is further amended by adding at the end the following new section:

''SEC. 603. ANNUAL REPORTS.

''(a) REPORT BY DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS.—

''(1) REPORT REQUIRED.—The Director of the Administrative Office of the United States Courts shall annually submit to the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate, subject to a declassification review by the Attorney General and the Director of National Intelligence, a report that includes—

''(A) the number of applications or certifications for orders submitted under each of sections 105, 304, 402, 501, 702, 703, and 704;

''(B) the number of such orders granted under each of those sections;

''(C) the number of orders modified under each of those sections;

''(D) the number of applications or certifications denied under each of those sections;

''(E) the number of appointments of an individual to serve as amicus curiae under section 103, including the name of each individual appointed to serve as amicus curiae; and

''(F) the number of findings issued under section 103(i) that such appointment is not appropriate and the text of any such findings.

''(2) PUBLICATION.—The Director shall make the report required under paragraph (1) publicly available on an Internet Web site, except that the Director shall not make publicly available on an Internet Web site the findings described in subparagraph (F) of paragraph (1).

''(b) MANDATORY REPORTING BY DIRECTOR OF NATIONAL INTELLIGENCE.—Except as provided in subsection (d), the Director of National Intelligence shall annually make publicly available on an Internet Web site a report that identifies, for the preceding 12-month period—

''(1) the total number of orders issued pursuant to titles I and III and sections 703 and 704 and a good faith estimate of the number of targets of such orders;

''(2) the total number of orders issued pursuant to section 702 and a good faith estimate of—

''(A) the number of search terms concerning a known United States person used to retrieve the unminimized contents of electronic communications or wire communications obtained through acquisitions authorized under such section, excluding the number of search terms used to prevent the return of information concerning a United States person; and

''(B) the number of queries concerning a known United States person of unminimized noncontents information relating to electronic communications or wire communications obtained through acquisitions authorized under such section, excluding the number of queries containing information used to prevent the return of information concerning a United States person;

''(3) the total number of orders issued pursuant to title IV and a good faith estimate of—

''(A) the number of targets of such orders; and

''(B) the number of unique identifiers used to communicate information collected pursuant to such orders;

''(4) the total number of orders issued pursuant to applications made under section 501(b)(2)(B) and a good faith estimate of—

''(A) the number of targets of such orders; and

''(B) the number of unique identifiers used to communicate information collected pursuant to such orders;

''(5) the total number of orders issued pursuant to applications made under section 501(b)(2)(C) and a good faith estimate of—

''(A) the number of targets of such orders;

''(B) the number of unique identifiers used to communicate information collected pursuant to such orders; and

''(C) the number of search terms that included information concerning a United States person that were used to query any database of call detail records obtained through the use of such orders; and

''(6) the total number of national security letters issued and the number of requests for information contained within such national security letters.

''(c) TIMING.—The annual reports required by subsections (a) and (b) shall be made publicly available during April of each year and include information relating to the previous calendar year.

''(d) EXCEPTIONS.—

''(1) STATEMENT OF NUMERICAL RANGE.—If a good faith estimate required to be reported under subparagraph (B) of any of paragraphs (3), (4), or (5) of subsection (b) is fewer than 500, it shall be expressed as a numerical range of 'fewer than 500' and shall not be expressed as an individual number.

''(2) NONAPPLICABILITY TO CERTAIN INFORMATION.—

''(A) FEDERAL BUREAU OF INVESTIGATION.—Paragraphs (2)(A), (2)(B), and (5)(C) of subsection (b) shall not apply to information or records held by, or queries conducted by, the Federal Bureau of Investigation.

''(B) ELECTRONIC MAIL ADDRESS AND TELEPHONE NUMBERS.—Paragraph (3)(B) of subsection (b) shall not apply to orders resulting in the acquisition of information by the Federal Bureau of Investigation that does not include electronic mail addresses or telephone numbers.

''(3) CERTIFICATION.—

''(A) IN GENERAL.—If the Director of National Intelligence concludes that a good faith estimate required to be reported under subsection (b)(2)(B) cannot be determined accurately because some but not all of the relevant elements of the intelligence community are able to provide such good faith estimate, the Director shall—

''(i) certify that conclusion in writing to the Select Committee on Intelligence and the Committee on the Judiciary of the Senate and the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives;

''(ii) report the good faith estimate for those relevant elements able to provide such good faith estimate;

''(iii) explain when it is reasonably anticipated that such an estimate will be able to be determined fully and accurately; and

''(iv) make such certification publicly available on an Internet Web site.

''(B) FORM.—A certification described in subparagraph (A) shall be prepared in unclassified form, but may contain a classified annex.

''(C) TIMING.—If the Director of National Intelligence continues to conclude that the good faith estimates described in this paragraph cannot be determined accurately, the Director shall annually submit a certification in accordance with this paragraph.

''(e) DEFINITIONS.—In this section:

''(1) CONTENTS.—The term 'contents' has the meaning given that term under section 2510 of title 18, United States Code.

''(2) ELECTRONIC COMMUNICATION.—The term 'electronic communication' has the meaning given that term under section 2510 of title 18, United States Code.

''(3) NATIONAL SECURITY LETTER.—The term 'national security letter' means a request for a report, records, or other information under—

''(A) section 2709 of title 18, United States Code;

''(B) section 1114(a)(5)(A) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(5)(A));

''(C) subsection (a) or (b) of section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u(a), 1681u(b)); or

''(D) section 627(a) of the Fair Credit Reporting Act (15 U.S.C. 1681v(a)).

''(4) UNITED STATES PERSON.—The term 'United States person' means a citizen of the United States or an alien lawfully admitted for permanent residence (as defined in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a))).

''(5) WIRE COMMUNICATION.—The term 'wire communication' has the meaning given that term under section 2510 of title 18, United States Code.''.

(b) TABLE OF CONTENTS AMENDMENT.—The table of contents, as amended by section 402 of this Act, is further amended by inserting after the item relating to section 602, as added by section 402 of this Act, the following new item:

''Sec. 603. Annual reports.''.

(c) PUBLIC REPORTING ON NATIONAL SECURITY LETTERS.—Section 118(c) of the USA PATRIOT Improvement and Reauthorization Act of 2005 (18 U.S.C. 3511 note) is amended—

(1) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking ''United States''; and

(B) in subparagraph (A), by striking '', excluding the number of requests for subscriber information'';

(2) by redesignating paragraph (2) as paragraph (3); and

(3) by inserting after paragraph (1) the following:

''(2) CONTENT.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), each report required under this subsection shall include a good faith estimate of the total number of requests described in paragraph (1) requiring disclosure of information concerning—

''(i) United States persons; and

''(ii) persons who are not United States persons.

''(B) EXCEPTION.—With respect to the number of requests for subscriber information under section 2709 of title 18, United States Code, a report required under this subsection need not separate the number of requests into each of the categories described in subparagraph (A).''.

(d) STORED COMMUNICATIONS.—Section 2702(d) of title 18, United States Code, is amended—

(1) in paragraph (1), by striking ''; and'' and inserting a semicolon;

(2) in paragraph (2)(B), by striking the period and inserting ''; and''; and

(3) by adding at the end the following new paragraph:

''(3) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (c)(4).''.

SEC. 603. PUBLIC REPORTING BY PERSONS SUBJECT TO FISA ORDERS.

(a) IN GENERAL.—Title VI (50 U.S.C. 1871 et seq.), as amended by sections 402 and 602 of this Act, is further amended by adding at the end the following new section:

''SEC. 604. PUBLIC REPORTING BY PERSONS SUBJECT TO ORDERS.

''(a) REPORTING.—A person subject to a nondisclosure requirement accompanying an order or directive under this Act or a national security letter may, with respect to such order, directive, or national security letter, publicly report the following information using one of the following structures:

''(1) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply into separate categories of—

''(A) the number of national security letters received, reported in bands of 1000 starting with 0–999;

''(B) the number of customer selectors targeted by national security letters, reported in bands of 1000 starting with 0–999;

''(C) the number of orders or directives received, combined, under this Act for contents, reported in bands of 1000 starting with 0–999;

''(D) the number of customer selectors targeted under orders or directives received, combined, under this Act for contents reported in bands of 1000 starting with 0–999;

''(E) the number of orders received under this Act for noncontents, reported in bands of 1000 starting with 0–999; and

''(F) the number of customer selectors targeted under orders under this Act for noncontents, reported in bands of 1000 starting with 0–999, pursuant to—

''(i) title IV;

''(ii) title V with respect to applications described in section 501(b)(2)(B); and

''(iii) title V with respect to applications described in section 501(b)(2)(C).

''(2) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply into separate categories of—

''(A) the number of national security letters received, reported in bands of 500 starting with 0–499;

''(B) the number of customer selectors targeted by national security letters, reported in bands of 500 starting with 0–499;

''(C) the number of orders or directives received, combined, under this Act for contents, reported in bands of 500 starting with 0–499;

''(D) the number of customer selectors targeted under orders or directives received, combined, under this Act for contents, reported in bands of 500 starting with 0–499;

''(E) the number of orders received under this Act for noncontents, reported in bands of 500 starting with 0–499; and

''(F) the number of customer selectors targeted under orders received under this Act for noncontents, reported in bands of 500 starting with 0–499.

''(3) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply in the into separate categories of—

''(A) the total number of all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 250 starting with 0–249; and

''(B) the total number of customer selectors targeted under all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 250 starting with 0–249.

''(4) An annual report that aggregates the number of orders, directives, and national security letters the person was required to comply with into separate categories of—

''(A) the total number of all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 100 starting with 0–99; and

''(B) the total number of customer selectors targeted under all national security process received, including all national security letters, and orders or directives under

this Act, combined, reported in bands of 100 starting with 0–99.

''(b) PERIOD OF TIME COVERED BY REPORTS.—

''(1) A report described in paragraph (1) or (2) of subsection (a) shall include only information—

''(A) relating to national security letters for the previous 180 days; and

''(B) relating to authorities under this Act for the 180-day period of time ending on the date that is not less than 180 days prior to the date of the publication of such report, except that with respect to a platform, product, or service for which a person did not previously receive an order or directive (not including an enhancement to or iteration of an existing publicly available platform, product, or service) such report shall not include any information relating to such new order or directive until 540 days after the date on which such new order or directive is received.

''(2) A report described in paragraph (3) of subsection (a) shall include only information relating to the previous 180 days.

''(3) A report described in paragraph (4) of subsection (a) shall include only information for the 1-year period of time ending on the date that is not less than 1 year prior to the date of the publication of such report.

''(c) OTHER FORMS OF AGREED TO PUBLICATION.—Nothing in this section prohibits the Government and any person from jointly agreeing to the publication of information referred to in this subsection in a time, form, or manner other than as described in this section.

''(d) DEFINITIONS.—In this section:

''(1) CONTENTS.—The term 'contents' has the meaning given that term under section 2510 of title 18, United States Code.

''(2) NATIONAL SECURITY LETTER.—The term 'national security letter' has the meaning given that term under section 603.''.

(b) TABLE OF CONTENTS AMENDMENT.—The table of contents, as amended by sections 402 and 602 of this Act, is further amended by inserting after the item relating to section 603, as added by section 602 of this Act, the following new item:

''Sec. 604. Public reporting by persons subject to orders.''.

SEC. 604. REPORTING REQUIREMENTS FOR DECISIONS, ORDERS, AND OPINIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT AND THE FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW.

Section 601(c)(1) (50 U.S.C. 1871(c)(1)) is amended to read as follows:

''(1) not later than 45 days after the date on which the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review issues a decision, order, or opinion, including any denial or modification of an application under this Act, that includes significant construction or interpretation of any provision of law or results in a change of application of any provision of this Act or a novel application of any provision of this Act, a copy of such decision, order, or opinion and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion; and''.

SEC. 605. SUBMISSION OF REPORTS UNDER FISA.

(a) ELECTRONIC SURVEILLANCE.—Section 108(a)(1) (50 U.S.C. 1808(a)(1)) is amended by striking ''the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, and the Committee on the Judiciary of the Senate,'' and inserting ''the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate''.

(b) PHYSICAL SEARCHES.—The matter preceding paragraph (1) of section 306 (50 U.S.C. 1826) is amended—

(1) in the first sentence, by striking ''Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the Senate,'' and inserting ''Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate''; and

(2) in the second sentence, by striking ''and the Committee on the Judiciary of the House of Representatives''.

(c) PEN REGISTERS AND TRAP AND TRACE DEVICES.—Section 406(b) (50 U.S.C. 1846(b)) is amended—

(1) in paragraph (2), by striking ''; and'' and inserting a semicolon;

(2) in paragraph (3), by striking the period and inserting a semicolon; and

(3) by adding at the end the following new paragraphs:

''(4) each department or agency on behalf of which the Attorney General or a designated attorney for the Government has made an application for an order authorizing or approving the installation and use of a pen register or trap and trace device under this title; and

''(5) for each department or agency described in paragraph (4), each number described in paragraphs (1), (2), and (3).''.

(d) ACCESS TO CERTAIN BUSINESS RECORDS AND OTHER TANGIBLE THINGS.—Section 502(a) (50 U.S.C. 1862(a)) is amended by striking ''Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate'' and inserting ''Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate''.

TITLE VII—ENHANCED NATIONAL SECURITY PROVISIONS

SEC. 701. EMERGENCIES INVOLVING NON-UNITED STATES PERSONS.

(a) IN GENERAL.—Section 105 (50 U.S.C. 1805) is amended—

(1) by redesignating subsections (f), (g), (h), and (i) as subsections (g), (h), (i), and (j), respectively; and

(2) by inserting after subsection (e) the following:

''(f)(1) Notwithstanding any other provision of this Act, the lawfully authorized targeting of a non-United States person previously believed to be located outside the United States for the acquisition of foreign intelligence information may continue for a period not to exceed 72 hours from the time that the non-United States person is reasonably believed to be located inside the United States and the acquisition is subject to this title or to title III of this Act, provided that the head of an element of the intelligence community—

''(A) reasonably determines that a lapse in the targeting of such non-United States person poses a threat of death or serious bodily harm to any person;

''(B) promptly notifies the Attorney General of a determination under subparagraph (A); and

''(C) requests, as soon as practicable, the employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical search pursuant to section 304(e), as warranted.

''(2) The authority under this subsection to continue the acquisition of foreign intelligence information is limited to a period not to exceed 72 hours and shall cease upon the earlier of the following:

''(A) The employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical search pursuant to section 304(e).

''(B) An issuance of a court order under this title or title III of this Act.

''(C) The Attorney General provides direction that the acquisition be terminated.

''(D) The head of the element of the intelligence community conducting the acquisition determines that a request under paragraph (1)(C) is not warranted.

''(E) When the threat of death or serious bodily harm to any person is no longer reasonably believed to exist.

''(3) Nonpublicly available information concerning unconsenting United States persons acquired under this subsection shall not be disseminated during the 72 hour time period under paragraph (1) unless necessary to investigate, reduce, or eliminate the threat of death or serious bodily harm to any person.

''(4) If the Attorney General declines to authorize the employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical search pursuant to section 304(e), or a court order is not obtained under this title or title III of this Act, information obtained during the 72 hour acquisition time period under paragraph (1) shall not be retained, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

''(5) Paragraphs (5) and (6) of subsection (e) shall apply to this subsection.''.

(b) NOTIFICATION OF EMERGENCY EMPLOYMENT OF ELECTRONIC SURVEILLANCE.—Section 106(j) (50 U.S.C. 1806(j)) is amended by striking ''section 105(e)'' and inserting ''subsection (e) or (f) of section 105''.

(c) REPORT TO CONGRESS.—Section 108(a)(2) (50 U.S.C. 1808(a)(2)) is amended—

(1) in subparagraph (B), by striking ''and'' at the end;

(2) in subparagraph (C), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following:

''(D) the total number of authorizations under section 105(f) and the total number of subsequent emergency employments of electronic surveillance under section 105(e) or emergency physical searches pursuant to section 301(e).''.

SEC. 702. PRESERVATION OF TREATMENT OF NON-UNITED STATES PERSONS TRAVELING OUTSIDE THE UNITED STATES AS AGENTS OF FOREIGN POWERS.

Section 101(b)(1) is amended—

(1) in subparagraph (A), by inserting before the semicolon at the end the following: '', irrespective of whether the person is inside the United States''; and

(2) in subparagraph (B)—

(A) by striking ''of such person's presence in the United States''; and

(B) by striking ''such activities in the United States'' and inserting ''such activities''.

SEC. 703. IMPROVEMENT TO INVESTIGATIONS OF INTERNATIONAL PROLIFERATION OF WEAPONS OF MASS DESTRUCTION.

Section 101(b)(1) is further amended by striking subparagraph (E) and inserting the following new subparagraph (E):

''(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power, or knowingly aids or abets any person in the conduct of such proliferation or activities in preparation therefor, or knowingly conspires with any person

to engage in such proliferation or activities in preparation therefor; or''.

SEC. 704. INCREASE IN PENALTIES FOR MATERIAL SUPPORT OF FOREIGN TERRORIST ORGANIZATIONS.

Section 2339B(a)(1) of title 18, United States Code, is amended by striking ''15 years'' and inserting ''20 years''.

SEC. 705. SUNSETS.

(a) USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT OF 2005.—Section 102(b)(1) of the USA PATRIOT Improvement and Reauthorization Act of 2005 (50 U.S.C. 1805 note) is amended by striking ''June 1, 2015'' and inserting ''December 15, 2019''.

(b) INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004.—Section 6001(b)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 1801 note) is amended by striking ''June 1, 2015'' and inserting ''December 15, 2019''.

(c) CONFORMING AMENDMENT.—Section 102(b)(1) of the USA PATRIOT Improvement and Reauthorization Act of 2005 (50 U.S.C. 1805 note), as amended by subsection (a), is further amended by striking ''sections 501, 502, and'' and inserting ''title V and section''.

TITLE VIII—SAFETY OF MARITIME NAVIGATION AND NUCLEAR TERRORISM CONVENTIONS IMPLEMENTATION

Subtitle A—Safety of Maritime Navigation

SEC. 801. AMENDMENT TO SECTION 2280 OF TITLE 18, UNITED STATES CODE.

Section 2280 of title 18, United States Code, is amended—

(1) in subsection (b)—

(A) in paragraph (1)(A)(i), by striking ''a ship flying the flag of the United States'' and inserting ''a vessel of the United States or a vessel subject to the jurisdiction of the United States (as defined in section 70502 of title 46)'';

(B) in paragraph (1)(A)(ii), by inserting '', including the territorial seas'' after ''in the United States''; and

(C) in paragraph (1)(A)(iii), by inserting '', by a United States corporation or legal entity,'' after ''by a national of the United States'';

(2) in subsection (c), by striking ''section 2(c)'' and inserting ''section 13(c)'';

(3) by striking subsection (d);

(4) by striking subsection (e) and inserting after subsection (c) the following:

''(d) DEFINITIONS.—As used in this section, section 2280a, section 2281, and section 2281a, the term—

''(1) 'applicable treaty' means—

''(A) the Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16 December 1970;

''(B) the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 23 September 1971;

''(C) the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on 14 December 1973;

''(D) International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on 17 December 1979;

''(E) the Convention on the Physical Protection of Nuclear Material, done at Vienna on 26 October 1979;

''(F) the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 24 February 1988;

''(G) the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, done at Rome on 10 March 1988;

''(H) International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997; and

''(I) International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations on 9 December 1999;

''(2) 'armed conflict' does not include internal disturbances and tensions, such as riots, isolated and sporadic acts of violence, and other acts of a similar nature;

''(3) 'biological weapon' means—

''(A) microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective, or other peaceful purposes; or

''(B) weapons, equipment, or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict;

''(4) 'chemical weapon' means, together or separately—

''(A) toxic chemicals and their precursors, except where intended for—

''(i) industrial, agricultural, research, medical, pharmaceutical, or other peaceful purposes;

''(ii) protective purposes, namely those purposes directly related to protection against toxic chemicals and to protection against chemical weapons;

''(iii) military purposes not connected with the use of chemical weapons and not dependent on the use of the toxic properties of chemicals as a method of warfare; or

''(iv) law enforcement including domestic riot control purposes,

as long as the types and quantities are consistent with such purposes;

''(B) munitions and devices, specifically designed to cause death or other harm through the toxic properties of those toxic chemicals specified in subparagraph (A), which would be released as a result of the employment of such munitions and devices; and

''(C) any equipment specifically designed for use directly in connection with the employment of munitions and devices specified in subparagraph (B);

''(5) 'covered ship' means a ship that is navigating or is scheduled to navigate into, through or from waters beyond the outer limit of the territorial sea of a single country or a lateral limit of that country's territorial sea with an adjacent country;

''(6) 'explosive material' has the meaning given the term in section 841(c) and includes explosive as defined in section 844(j) of this title;

''(7) 'infrastructure facility' has the meaning given the term in section 2332f(e)(5) of this title;

''(8) 'international organization' has the meaning given the term in section 831(f)(3) of this title;

''(9) 'military forces of a state' means the armed forces of a state which are organized, trained, and equipped under its internal law for the primary purpose of national defense or security, and persons acting in support of those armed forces who are under their formal command, control, and responsibility;

''(10) 'national of the United States' has the meaning stated in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22));

''(11) 'Non-Proliferation Treaty' means the Treaty on the Non-Proliferation of Nuclear Weapons, done at Washington, London, and Moscow on 1 July 1968;

''(12) 'Non-Proliferation Treaty State Party' means any State Party to the Non-Proliferation Treaty, to include Taiwan, which shall be considered to have the obligations under the Non-Proliferation Treaty of a party to that treaty other than a Nuclear Weapon State Party to the Non-Proliferation Treaty;

''(13) 'Nuclear Weapon State Party to the Non-Proliferation Treaty' means a State Party to the Non-Proliferation Treaty that is a nuclear-weapon State, as that term is defined in Article IX(3) of the Non-Proliferation Treaty;

''(14) 'place of public use' has the meaning given the term in section 2332f(e)(6) of this title;

''(15) 'precursor' has the meaning given the term in section 229F(6)(A) of this title;

''(16) 'public transport system' has the meaning given the term in section 2332f(e)(7) of this title;

''(17) 'serious injury or damage' means—

''(A) serious bodily injury,

''(B) extensive destruction of a place of public use, State or government facility, infrastructure facility, or public transportation system, resulting in major economic loss, or

''(C) substantial damage to the environment, including air, soil, water, fauna, or flora;

''(18) 'ship' means a vessel of any type whatsoever not permanently attached to the sea-bed, including dynamically supported craft, submersibles, or any other floating craft, but does not include a warship, a ship owned or operated by a government when being used as a naval auxiliary or for customs or police purposes, or a ship which has been withdrawn from navigation or laid up;

''(19) 'source material' has the meaning given that term in the International Atomic Energy Agency Statute, done at New York on 26 October 1956;

''(20) 'special fissionable material' has the meaning given that term in the International Atomic Energy Agency Statute, done at New York on 26 October 1956;

''(21) 'territorial sea of the United States' means all waters extending seaward to 12 nautical miles from the baselines of the United States determined in accordance with international law;

''(22) 'toxic chemical' has the meaning given the term in section 229F(8)(A) of this title;

''(23) 'transport' means to initiate, arrange or exercise effective control, including decisionmaking authority, over the movement of a person or item; and

''(24) 'United States', when used in a geographical sense, includes the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, and all territories and possessions of the United States.''; and

(5) by inserting after subsection (d) (as added by paragraph (4) of this section) the following:

''(e) EXCEPTIONS.—This section shall not apply to—

''(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

''(2) activities undertaken by military forces of a state in the exercise of their official duties.

''(f) DELIVERY OF SUSPECTED OFFENDER.—The master of a covered ship flying the flag of the United States who has reasonable grounds to believe that there is on board that ship any person who has committed an offense under section 2280 or section 2280a may deliver such person to the authorities of a country that is a party to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation. Before delivering such person to the authorities of another country, the master shall notify in an appropriate manner the Attorney General of the United States of the alleged offense and await instructions from the Attorney

General as to what action to take. When delivering the person to a country which is a state party to the Convention, the master shall, whenever practicable, and if possible before entering the territorial sea of such country, notify the authorities of such country of the master's intention to deliver such person and the reasons therefor. If the master delivers such person, the master shall furnish to the authorities of such country the evidence in the master's possession that pertains to the alleged offense.

''(g)(1) CIVIL FORFEITURE.—Any real or personal property used or intended to be used to commit or to facilitate the commission of a violation of this section, the gross proceeds of such violation, and any real or personal property traceable to such property or proceeds, shall be subject to forfeiture.

''(2) APPLICABLE PROCEDURES.—Seizures and forfeitures under this section shall be governed by the provisions of chapter 46 of title 18, United States Code, relating to civil forfeitures, except that such duties as are imposed upon the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents, and other persons as may be designated for that purpose by the Secretary of Homeland Security, the Attorney General, or the Secretary of Defense.''.

SEC. 802. NEW SECTION 2280A OF TITLE 18, UNITED STATES CODE.

(a) IN GENERAL.—Chapter 111 of title 18, United States Code, is amended by adding after section 2280 the following new section:

''§ 2280a. Violence against maritime navigation and maritime transport involving weapons of mass destruction

''(a) OFFENSES.—

''(1) IN GENERAL.—Subject to the exceptions in subsection (c), a person who unlawfully and intentionally—

''(A) when the purpose of the act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act—

''(i) uses against or on a ship or discharges from a ship any explosive or radioactive material, biological, chemical, or nuclear weapon or other nuclear explosive device in a manner that causes or is likely to cause death to any person or serious injury or damage;

''(ii) discharges from a ship oil, liquefied natural gas, or another hazardous or noxious substance that is not covered by clause (i), in such quantity or concentration that causes or is likely to cause death to any person or serious injury or damage; or

''(iii) uses a ship in a manner that causes death to any person or serious injury or damage;

''(B) transports on board a ship—

''(i) any explosive or radioactive material, knowing that it is intended to be used to cause, or in a threat to cause, death to any person or serious injury or damage for the purpose of intimidating a population, or compelling a government or an international organization to do or to abstain from doing any act;

''(ii) any biological, chemical, or nuclear weapon or other nuclear explosive device, knowing it to be a biological, chemical, or nuclear weapon or other nuclear explosive device;

''(iii) any source material, special fissionable material, or equipment or material especially designed or prepared for the processing, use, or production of special fissionable material, knowing that it is intended to be used in a nuclear explosive activity or in any other nuclear activity not under safeguards pursuant to an International Atomic Energy Agency comprehensive safeguards agreement, except where—

''(I) such item is transported to or from the territory of, or otherwise under the control of, a Non-Proliferation Treaty State Party; and

''(II) the resulting transfer or receipt (including internal to a country) is not contrary to the obligations under the Non-Proliferation Treaty of the Non-Proliferation Treaty State Party from which, to the territory of which, or otherwise under the control of which such item is transferred;

''(iv) any equipment, materials, or software or related technology that significantly contributes to the design or manufacture of a nuclear weapon or other nuclear explosive device, with the intention that it will be used for such purpose, except where—

''(I) the country to the territory of which or under the control of which such item is transferred is a Nuclear Weapon State Party to the Non-Proliferation Treaty; and

''(II) the resulting transfer or receipt (including internal to a country) is not contrary to the obligations under the Non-Proliferation Treaty of a Non-Proliferation Treaty State Party from which, to the territory of which, or otherwise under the control of which such item is transferred;

''(v) any equipment, materials, or software or related technology that significantly contributes to the delivery of a nuclear weapon or other nuclear explosive device, with the intention that it will be used for such purpose, except where—

''(I) such item is transported to or from the territory of, or otherwise under the control of, a Non-Proliferation Treaty State Party; and

''(II) such item is intended for the delivery system of a nuclear weapon or other nuclear explosive device of a Nuclear Weapon State Party to the Non-Proliferation Treaty; or

''(vi) any equipment, materials, or software or related technology that significantly contributes to the design, manufacture, or delivery of a biological or chemical weapon, with the intention that it will be used for such purpose;

''(C) transports another person on board a ship knowing that the person has committed an act that constitutes an offense under section 2280 or subparagraph (A), (B), (D), or (E) of this section or an offense set forth in an applicable treaty, as specified in section 2280(d)(1), and intending to assist that person to evade criminal prosecution;

''(D) injures or kills any person in connection with the commission or the attempted commission of any of the offenses set forth in subparagraphs (A) through (C), or subsection (a)(2), to the extent that the subsection (a)(2) offense pertains to subparagraph (A); or

''(E) attempts to do any act prohibited under subparagraph (A), (B) or (D), or conspires to do any act prohibited by subparagraphs (A) through (E) or subsection (a)(2),

shall be fined under this title, imprisoned not more than 20 years, or both; and if the death of any person results from conduct prohibited by this paragraph, shall be imprisoned for any term of years or for life.

''(2) THREATS.—A person who threatens, with apparent determination and will to carry the threat into execution, to do any act prohibited under paragraph (1)(A) shall be fined under this title, imprisoned not more than 5 years, or both.

''(b) JURISDICTION.—There is jurisdiction over the activity prohibited in subsection (a)—

''(1) in the case of a covered ship, if—

''(A) such activity is committed—

''(i) against or on board a vessel of the United States or a vessel subject to the jurisdiction of the United States (as defined in section 70502 of title 46) at the time the prohibited activity is committed;

''(ii) in the United States, including the territorial seas; or

''(iii) by a national of the United States, by a United States corporation or legal entity, or by a stateless person whose habitual residence is in the United States;

''(B) during the commission of such activity, a national of the United States is seized, threatened, injured, or killed; or

''(C) the offender is later found in the United States after such activity is committed;

''(2) in the case of a ship navigating or scheduled to navigate solely within the territorial sea or internal waters of a country other than the United States, if the offender is later found in the United States after such activity is committed; or

''(3) in the case of any vessel, if such activity is committed in an attempt to compel the United States to do or abstain from doing any act.

''(c) EXCEPTIONS.—This section shall not apply to—

''(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

''(2) activities undertaken by military forces of a state in the exercise of their official duties.

''(d)(1) CIVIL FORFEITURE.—Any real or personal property used or intended to be used to commit or to facilitate the commission of a violation of this section, the gross proceeds of such violation, and any real or personal property traceable to such property or proceeds, shall be subject to forfeiture.

''(2) APPLICABLE PROCEDURES.—Seizures and forfeitures under this section shall be governed by the provisions of chapter 46 of title 18, United States Code, relating to civil forfeitures, except that such duties as are imposed upon the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents, and other persons as may be designated for that purpose by the Secretary of Homeland Security, the Attorney General, or the Secretary of Defense.''.

(b) CONFORMING AMENDMENT.—The table of sections at the beginning of chapter 111 of title 18, United States Code, is amended by adding after the item relating to section 2280 the following new item:

''2280a. Violence against maritime navigation and maritime transport involving weapons of mass destruction.''.

SEC. 803. AMENDMENTS TO SECTION 2281 OF TITLE 18, UNITED STATES CODE.

Section 2281 of title 18, United States Code, is amended—

(1) in subsection (c), by striking ''section 2(c)'' and inserting ''section 13(c)'';

(2) in subsection (d), by striking the definitions of ''national of the United States,'' ''territorial sea of the United States,'' and ''United States''; and

(3) by inserting after subsection (d) the following:

''(e) EXCEPTIONS.—This section does not apply to—

''(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

''(2) activities undertaken by military forces of a state in the exercise of their official duties.''.

SEC. 804. NEW SECTION 2281A OF TITLE 18, UNITED STATES CODE.

(a) IN GENERAL.—Chapter 111 of title 18, United States Code, is amended by adding after section 2281 the following new section:

''§ 2281a. Additional offenses against maritime fixed platforms

''(a) OFFENSES.—

''(1) IN GENERAL.—A person who unlawfully and intentionally—

''(A) when the purpose of the act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act—

''(i) uses against or on a fixed platform or discharges from a fixed platform any explosive or radioactive material, biological, chemical, or nuclear weapon in a manner that causes or is likely to cause death or serious injury or damage; or

''(ii) discharges from a fixed platform oil, liquefied natural gas, or another hazardous or noxious substance that is not covered by clause (i), in such quantity or concentration that causes or is likely to cause death or serious injury or damage;

''(B) injures or kills any person in connection with the commission or the attempted commission of any of the offenses set forth in subparagraph (A); or

''(C) attempts or conspires to do anything prohibited under subparagraph (A) or (B),

shall be fined under this title, imprisoned not more than 20 years, or both; and if death results to any person from conduct prohibited by this paragraph, shall be imprisoned for any term of years or for life.

''(2) THREAT TO SAFETY.—A person who threatens, with apparent determination and will to carry the threat into execution, to do any act prohibited under paragraph (1)(A), shall be fined under this title, imprisoned not more than 5 years, or both.

''(b) JURISDICTION.—There is jurisdiction over the activity prohibited in subsection (a) if—

''(1) such activity is committed against or on board a fixed platform—

''(A) that is located on the continental shelf of the United States;

''(B) that is located on the continental shelf of another country, by a national of the United States or by a stateless person whose habitual residence is in the United States; or

''(C) in an attempt to compel the United States to do or abstain from doing any act;

''(2) during the commission of such activity against or on board a fixed platform located on a continental shelf, a national of the United States is seized, threatened, injured, or killed; or

''(3) such activity is committed against or on board a fixed platform located outside the United States and beyond the continental shelf of the United States and the offender is later found in the United States.

''(c) EXCEPTIONS.—This section does not apply to—

''(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

''(2) activities undertaken by military forces of a state in the exercise of their official duties.

''(d) DEFINITIONS.—In this section—

''(1) 'continental shelf' means the sea-bed and subsoil of the submarine areas that extend beyond a country's territorial sea to the limits provided by customary international law as reflected in Article 76 of the 1982 Convention on the Law of the Sea; and

''(2) 'fixed platform' means an artificial island, installation, or structure permanently attached to the sea-bed for the purpose of exploration or exploitation of resources or for other economic purposes.''.

(b) CONFORMING AMENDMENT.—The table of sections at the beginning of chapter 111 of title 18, United States Code, is amended by adding after the item relating to section 2281 the following new item:

''2281a. Additional offenses against maritime fixed platforms.''.

SEC. 805. ANCILLARY MEASURE.

Section 2332b(g)(5)(B) of title 18, United States Code, is amended by inserting ''2280a (relating to maritime safety),'' before ''2281'', and by striking ''2281'' and inserting ''2281 through 2281a''.

Subtitle B—Prevention of Nuclear Terrorism

SEC. 811. NEW SECTION 2332I OF TITLE 18, UNITED STATES CODE.

(a) IN GENERAL.—Chapter 113B of title 18, United States Code, is amended by adding after section 2332h the following:

''§ 2332i. Acts of nuclear terrorism

''(a) OFFENSES.—

''(1) IN GENERAL.—Whoever knowingly and unlawfully—

''(A) possesses radioactive material or makes or possesses a device—

''(i) with the intent to cause death or serious bodily injury; or

''(ii) with the intent to cause substantial damage to property or the environment; or

''(B) uses in any way radioactive material or a device, or uses or damages or interferes with the operation of a nuclear facility in a manner that causes the release of or increases the risk of the release of radioactive material, or causes radioactive contamination or exposure to radiation—

''(i) with the intent to cause death or serious bodily injury or with the knowledge that such act is likely to cause death or serious bodily injury;

''(ii) with the intent to cause substantial damage to property or the environment or with the knowledge that such act is likely to cause substantial damage to property or the environment; or

''(iii) with the intent to compel a person, an international organization or a country to do or refrain from doing an act,

shall be punished as prescribed in subsection (c).

''(2) THREATS.—Whoever, under circumstances in which the threat may reasonably be believed, threatens to commit an offense under paragraph (1) shall be punished as prescribed in subsection (c). Whoever demands possession of or access to radioactive material, a device or a nuclear facility by threat or by use of force shall be punished as prescribed in subsection (c).

''(3) ATTEMPTS AND CONSPIRACIES.—Whoever attempts to commit an offense under paragraph (1) or conspires to commit an offense under paragraph (1) or (2) shall be punished as prescribed in subsection (c).

''(b) JURISDICTION.—Conduct prohibited by subsection (a) is within the jurisdiction of the United States if—

''(1) the prohibited conduct takes place in the United States or the special aircraft jurisdiction of the United States;

''(2) the prohibited conduct takes place outside of the United States and—

''(A) is committed by a national of the United States, a United States corporation or legal entity or a stateless person whose habitual residence is in the United States;

''(B) is committed on board a vessel of the United States or a vessel subject to the jurisdiction of the United States (as defined in section 70502 of title 46) or on board an aircraft that is registered under United States law, at the time the offense is committed; or

''(C) is committed in an attempt to compel the United States to do or abstain from doing any act, or constitutes a threat directed at the United States;

''(3) the prohibited conduct takes place outside of the United States and a victim or an intended victim is a national of the United States or a United States corporation or legal entity, or the offense is committed against any state or government facility of the United States; or

''(4) a perpetrator of the prohibited conduct is found in the United States.

''(c) PENALTIES.—Whoever violates this section shall be fined not more than $2,000,000 and shall be imprisoned for any term of years or for life.

''(d) NONAPPLICABILITY.—This section does not apply to—

''(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

''(2) activities undertaken by military forces of a state in the exercise of their official duties.

''(e) DEFINITIONS.—As used in this section, the term—

''(1) 'armed conflict' has the meaning given that term in section 2332f(e)(11) of this title;

''(2) 'device' means:

''(A) any nuclear explosive device; or

''(B) any radioactive material dispersal or radiation-emitting device that may, owing to its radiological properties, cause death, serious bodily injury or substantial damage to property or the environment;

''(3) 'international organization' has the meaning given that term in section 831(f)(3) of this title;

''(4) 'military forces of a state' means the armed forces of a country that are organized, trained and equipped under its internal law for the primary purpose of national defense or security and persons acting in support of those armed forces who are under their formal command, control and responsibility;

''(5) 'national of the United States' has the meaning given that term in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22));

''(6) 'nuclear facility' means:

''(A) any nuclear reactor, including reactors on vessels, vehicles, aircraft or space objects for use as an energy source in order to propel such vessels, vehicles, aircraft or space objects or for any other purpose;

''(B) any plant or conveyance being used for the production, storage, processing or transport of radioactive material; or

''(C) a facility (including associated buildings and equipment) in which nuclear material is produced, processed, used, handled, stored or disposed of, if damage to or interference with such facility could lead to the release of significant amounts of radiation or radioactive material;

''(7) 'nuclear material' has the meaning given that term in section 831(f)(1) of this title;

''(8) 'radioactive material' means nuclear material and other radioactive substances that contain nuclides that undergo spontaneous disintegration (a process accompanied by emission of one or more types of ionizing radiation, such as alpha-, beta-, neutron particles and gamma rays) and that may, owing to their radiological or fissile properties, cause death, serious bodily injury or substantial damage to property or to the environment;

''(9) 'serious bodily injury' has the meaning given that term in section 831(f)(4) of this title;

''(10) 'state' has the same meaning as that term has under international law, and includes all political subdivisions thereof;

''(11) 'state or government facility' has the meaning given that term in section 2332f(e)(3) of this title;

''(12) 'United States corporation or legal entity' means any corporation or other entity organized under the laws of the United States or any State, Commonwealth, territory, possession or district of the United States;

''(13) 'vessel' has the meaning given that term in section 1502(19) of title 33; and

''(14) 'vessel of the United States' has the meaning given that term in section 70502 of title 46.''.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 113B of title 18, United States Code, is amended by inserting after the item relating to section 2332h the following:

''2332i. Acts of nuclear terrorism.''.

(c) DISCLAIMER.—Nothing contained in this section is intended to affect the applicability of any other Federal or State law that might pertain to the underlying conduct.

(d) INCLUSION IN DEFINITION OF FEDERAL CRIMES OF TERRORISM.—Section 2332b(g)(5)(B) of title 18, United States Code, is amended by inserting ''2332i (relating to acts of nuclear terrorism),'' before ''2339 (relating to harboring terrorists)''.

SEC. 812. AMENDMENT TO SECTION 831 OF TITLE 18, UNITED STATES CODE.

Section 831 of title 18, United States Code, is amended—

(a) in subsection (a)—

(1) by redesignating paragraphs (3) through (8) as paragraphs (4) through (9);

(2) by inserting after paragraph (2) the following:

''(3) without lawful authority, intentionally carries, sends or moves nuclear material into or out of a country;'';

(3) in paragraph (8), as redesignated, by striking ''an offense under paragraph (1), (2), (3), or (4)'' and inserting ''any act prohibited under paragraphs (1) through (5)''; and

(4) in paragraph (9), as redesignated, by striking ''an offense under paragraph (1), (2), (3), or (4)'' and inserting ''any act prohibited under paragraphs (1) through (7)'';

(b) in subsection (b)—

(1) in paragraph (1), by striking ''(7)'' and inserting ''(8)''; and

(2) in paragraph (2), by striking ''(8)'' and inserting ''(9)'';

(c) in subsection (c)—

(1) in subparagraph (2)(A), by adding after ''United States'' the following: ''or a stateless person whose habitual residence is in the United States'';

(2) by striking paragraph (5);

(3) in paragraph (4), by striking ''or'' at the end; and

(4) by inserting after paragraph (4), the following:

''(5) the offense is committed on board a vessel of the United States or a vessel subject to the jurisdiction of the United States (as defined in section 70502 of title 46) or on board an aircraft that is registered under United States law, at the time the offense is committed;

''(6) the offense is committed outside the United States and against any state or government facility of the United States; or

''(7) the offense is committed in an attempt to compel the United States to do or abstain from doing any act, or constitutes a threat directed at the United States.'';

(d) by redesignating subsections (d) through (f) as (e) through (g), respectively;

(e) by inserting after subsection (c) the following:

''(d) NONAPPLICABILITY.—This section does not apply to—

''(1) the activities of armed forces during an armed conflict, as those terms are understood under the law of war, which are governed by that law; or

''(2) activities undertaken by military forces of a state in the exercise of their official duties.''; and

(f) in subsection (g), as redesignated—

(1) in paragraph (6), by striking ''and'' at the end;

(2) in paragraph (7), by striking the period at the end and inserting a semicolon; and

(3) by inserting after paragraph (7), the following:

''(8) the term 'armed conflict' has the meaning given that term in section 2332f(e)(11) of this title;

''(9) the term 'military forces of a state' means the armed forces of a country that are organized, trained and equipped under its internal law for the primary purpose of national defense or security and persons acting in support of those armed forces who are under their formal command, control and responsibility;

''(10) the term 'state' has the same meaning as that term has under international law, and includes all political subdivisions thereof;

''(11) the term 'state or government facility' has the meaning given that term in section 2332f(e)(3) of this title; and

''(12) the term 'vessel of the United States' has the meaning given that term in section 70502 of title 46.''.

SA 1453. Mr. MCCONNELL proposed an amendment to amendment SA 1452 proposed by Mr. MCCONNELL (for himself and Mr. BURR) to the bill H.R. 2048, to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes; as follows:

At the end of the amendment, add the following:

''This Act shall take effect 1 day after the date of enactment.''

EXPRESSING APPRECIATION OF THE GOALS OF AMERICAN CRAFT BEER WEEK

Mr. MCCONNELL. Madam President, I ask unanimous consent that the Senate proceed to the immediate consideration of S. Res. 188, submitted earlier today.

The PRESIDING OFFICER. The clerk will report the resolution by title.

The legislative clerk read as follows:

A resolution (S. Res. 188) expressing appreciation of the goals of American Craft Beer Week and commending the small and independent craft brewers of the United States.

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

Mr. MCCONNELL. Madam President, I ask unanimous consent that the resolution be agreed to, the preamble be agreed to, and the motions to reconsider be made and laid upon the table with no intervening action or debate.

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

The resolution (S. Res. 188) was agreed to.

The preamble was agreed to.

(The resolution, with its preamble, is printed in today's RECORD under ''Submitted Resolutions.'')

EXECUTIVE SESSION

EXECUTIVE CALENDAR

Mr. MCCONNELL. Madam President, I ask unanimous consent that the Senate proceed to executive session to consider the following nominations en bloc: Calendar Nos. 95 and 125; that the nominations be confirmed, the motions to reconsider be considered made and laid upon the table with no intervening action or debate; that no further motions be in order; that any statements related to the nominations be printed in the RECORD; that the President be immediately notified of the Senate's actions, and the Senate then resume legislative session.

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

The nominations considered and confirmed en bloc are as follows:

IN THE AIR FORCE

The following named officer for appointment as Vice Chief of Staff, United States Air Force, and appointment in the United States Air Force to the grade indicated while assigned to a position of importance and responsibility under title 10, U.S.C., sections 8034 and 601:

To be general

Lt. Gen. David L. Goldfein

IN THE COAST GUARD

The following officer for appointment in the United States Coast Guard to the grade indicated while assigned to a position of importance and responsibility as Deputy Commandant for Mission Support under title 14, U.S.C., section 50:

To be vice admiral

Rear Adm. Sandra L. Stosz

LEGISLATIVE SESSION

The PRESIDING OFFICER. The Senate will now resume legislative session.

ORDERS FOR MONDAY, JUNE 1, 2015

Mr. MCCONNELL. Madam President, I ask unanimous consent that when the Senate completes its business today, it adjourn until 12 noon on Monday, June 1; 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 for up to 10 minutes each; finally, that following morning business, the Senate then resume consideration of H.R. 2048.

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

ADJOURNMENT UNTIL TOMORROW

Mr. MCCONNELL. 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 9:44 p.m., adjourned until Monday, June 1, 2015, at 12 noon.

CONFIRMATIONS

Executive nominations confirmed by the Senate May 31, 2015:

IN THE AIR FORCE

THE FOLLOWING NAMED OFFICER FOR APPOINTMENT AS VICE CHIEF OF STAFF, UNITED STATES AIR FORCE, AND APPOINTMENT IN THE UNITED STATES AIR FORCE TO THE GRADE INDICATED WHILE ASSIGNED TO A POSITION OF IMPORTANCE AND RESPONSIBILITY UNDER TITLE 10, U.S.C., SECTIONS 8034 AND 601:

To be general

LT. GEN. DAVID L. GOLDFEIN

IN THE COAST GUARD

THE FOLLOWING OFFICER FOR APPOINTMENT IN THE UNITED STATES COAST GUARD TO THE GRADE INDICATED WHILE ASSIGNED TO A POSITION OF IMPORTANCE AND RESPONSIBILITY AS DEPUTY COMMANDANT FOR MISSION SUPPORT UNDER TITLE 14, U.S.C., SECTION 50:

To be vice admiral

REAR ADM. SANDRA L. STOSZ