S. RES. 522

At the request of Mr. COONS, the names of the Senator from Illinois (Mr. DURBIN) and the Senator from New Hampshire (Mrs. SHAHEEN) were added as cosponsors of S. Res. 522, a resolution expressing the sense of the Senate supporting the U.S.-Africa Leaders Summit to be held in Washington, D.C. from August 4 through 6, 2014.

AMENDMENT NO. 3585

At the request of Mr. TOOMEY, the name of the Senator from Kentucky (Mr. MCCONNELL) was added as a cosponsor of amendment No. 3585 proposed to H.R. 5021, a bill 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.

AMENDMENT NO. 3626

At the request of Mr. BLUNT, the name of the Senator from Kentucky (Mr. MCCONNELL) was added as a cosponsor of amendment No. 3626 intended to be proposed to S. 2569, a bill to provide an incentive for businesses to bring jobs back to America.

AMENDMENT NO. 3629

At the request of Mr. BLUNT, the name of the Senator from Kentucky (Mr. MCCONNELL) was added as a cosponsor of amendment No. 3629 intended to be proposed to S. 2569, a bill to provide an incentive for businesses to bring jobs back to America.

AMENDMENT NO. 3630

At the request of Mr. PAUL, the name of the Senator from New Jersey (Mr. BOOKER) was added as a cosponsor of amendment No. 3630 intended to be proposed to S. 2569, a bill to provide an incentive for businesses to bring jobs back to America.

AMENDMENT NO. 3631

At the request of Mr. BARRASSO, the name of the Senator from Kentucky (Mr. MCCONNELL) was added as a cosponsor of amendment No. 3631 intended to be proposed to S. 2569, a bill to provide an incentive for businesses to bring jobs back to America.

AMENDMENT NO. 3632

At the request of Mr. THUNE, the name of the Senator from Kentucky (Mr. MCCONNELL) was added as a cosponsor of amendment No. 3632 intended to be proposed to S. 2569, a bill to provide an incentive for businesses to bring jobs back to America.

AMENDMENT NO. 3633

At the request of Mr. THUNE, the name of the Senator from Kentucky (Mr. MCCONNELL) was added as a cosponsor of amendment No. 3633 intended to be proposed to S. 2569, a bill to provide an incentive for businesses to bring jobs back to America.

AMENDMENT NO. 3635

At the request of Mr. THUNE, the name of the Senator from Kentucky (Mr. MCCONNELL) was added as a cosponsor of amendment No. 3635 intended to be proposed to S. 2569, a bill to provide an incentive for businesses to bring jobs back to America.

AMENDMENT NO. 3636

At the request of Mr. THUNE, the name of the Senator from Kentucky (Mr. MCCONNELL) was added as a cosponsor of amendment No. 3636 intended to be proposed to S. 2569, a bill to provide an incentive for businesses to bring jobs back to America.

AMENDMENT NO. 3656

At the request of Mr. HATCH, the name of the Senator from Kentucky (Mr. MCCONNELL) was added as a cosponsor of amendment No. 3656 intended to be proposed to S. 2569, a bill to provide an incentive for businesses to bring jobs back to America.

AMENDMENT NO. 3657

At the request of Mr. HATCH, the name of the Senator from Kentucky (Mr. MCCONNELL) was added as a cosponsor of amendment No. 3657 intended to be proposed to S. 2569, a bill to provide an incentive for businesses to bring jobs back to America.

AMENDMENT NO. 3687

At the request of Ms. COLLINS, the name of the Senator from Kentucky (Mr. MCCONNELL) was added as a cosponsor of amendment No. 3687 intended to be proposed to S. 2569, a bill to provide an incentive for businesses to bring jobs back to America.

AMENDMENT NO. 3698

At the request of Mr. ENZI, the name of the Senator from Minnesota (Mr. FRANKEN) was added as a cosponsor of amendment No. 3698 intended to be proposed to S. 2569, a bill to provide an incentive for businesses to bring jobs back to America.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. BOOKER (for himself, Mr. MENENDEZ, and Mrs. BOXER):

S. 2679. A bill to amend the Internal Revenue Code of 1986 to reinstate the financing for the Hazardous Substance Superfund, and for other purposes; to the Committee on Finance.

Mr. BOOKER. Mr. President, I rise today to introduce with my colleagues Senator ROBERT MENENDEZ of New Jersey, and Senator BARBARA BOXER of California, the Superfund Polluter Pays Restoration Act of 2014. This bill reinstates an expired excise tax on polluting industries to help fund the cleanup of Superfund sites and restore communities back to health.

Across our Nation we have far too many un-remediated and dangerous Superfund sites sitting in our neighborhoods—properties that are literally poisoning our residents. This problem is particularly acute in my State of New Jersey, which is both the most densely populated State and the State with the most Superfund sites.

Nationwide, there are more than 1300 Superfund sites on the National Priorities List, NPL, which require long-term cleanups. The sites listed on the NPL are the most heavily contaminated in the country and are the sites that pose the greatest potential risk to public health and the environment. In the past five years, 94 new sites have been added to the NPL, but an average of only 7 have been removed each year.

Cleanup has not even begun at hundreds of these NPL sites. Officials at the Environmental Protection Agency, EPA, and the Government Accountability Office, GAO, state that the reason why cleanup is not starting at hundreds of sites, and taking so long at others, is because of the limited funding available for cleanup activities.

There are more than 11 million Americans who live within one mile of a Superfund site, and of that, 3 to 4 million are children. Studies show that children are particularly susceptible to the health hazards presented by Superfund sites. Researchers have found increased autism rates, and recently researchers found that babies born to mothers living within 1 mile of a Superfund site prior to cleanup had a 20 percent greater incidence of being born with birth defects.

The need for more funding could not be clearer.

When Congress created Superfund in 1980, it established the Superfund Trust Fund from which the EPA receives annual appropriations for Superfund cleanup activities. For 15 years, the Trust Fund received a steady source of revenue from excise taxes on crude oil and certain chemicals. Those taxes expired at the end of fiscal year 1995. The Superfund program is now operating at 40 percent of 1987 levels, which is unsustainable according to a 2010 GAO report which found that current funding levels would likely not be sufficient to meet the future needs of the Superfund program EPA officials estimate they will need 2 to 2.5 times more funding to effectively and efficiently cleanup unremediated sites.

It is unfair for the taxpayer to shoulder the burden of cleanup costs for these Superfund sites. To meet the need for additional funding and to protect the health of our families and children, Senator MENENDEZ, Senator BOXER, and I have come together to introduce this act, aimed at holding polluting industries accountable, reducing the need to spend taxpayer dollars, and providing a steady flow of funds to the Superfund program.

By Mr. LEAHY (for himself, Mr. LEE, Mr. DURBIN, Mr. HELLER, Mr. FRANKEN, Mr. CRUZ, Mr. BLUMENTHAL, Mr. UDALL of New Mexico, Mr. COONS, Mr. HEINRICH, Mr. MARKEY, Ms. HIRONO, Ms. KLOBUCHAR, Mr. WHITEHOUSE, Mr. SCHUMER, and Mr. SANDERS):

S. 2685. 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; read the first time.

Mr. LEAHY. Mr. President, I am going to speak on another issue. I see my distinguished colleague from Utah Senator LEE is on the floor. It is an issue he has worked with me on. We have tried to join together. It was more than a year ago that not only here in the United States but the whole world learned some very startling details about the massive scope of the National Security Agency's surveillance programs.

Since then the American people, and actually, all three branches of government have been debating the same fundamental questions about the extent of government power that the Framers considered when they crafted the Constitution. Many of us had been arguing those same issues, whether in the Judiciary Committee, the Intelligence Committee, or others. But it was hard to get anybody's attention.

Suddenly the whole world was listening.

The obvious question is, when and how should the government be permitted to gather information about its citizens? How do we protect our country while we preserve our fundamental principles and our constitutional liberties? These questions are even more relevant and more complex as technology develops rapidly, and as more data is created every second.

Nobody questions that the government cannot just walk into our houses, rifle through our drawers, our filing cabinets, and our cupboards, to see what we might have there. But that is not where we keep our data anymore. It is on computers. By the same token, they shouldn't have the right to rifle through our electronic files either. If they collect all this data, should the government be allowed to collect and use all of it?

To what extent does this massive collection of data improve our national security and at what cost to our privacy and free expression? If we pick up everything, do we actually have anything?

The Senate Judiciary Committee considered these and other important questions during the course of six public hearings held over the past year. During this deliberative process, the Committee considered whether the bulk collection of Americans' phone records has been effective in preventing terrorist attacks, the privacy implications of the program, and the effect on the U.S. technology industry. Those hearings helped to demonstrate the need for additional limits on government surveillance authorities.

As these hearings continued, the call for an end to bulk collection under Section 215 of the USA PATRIOT Act grew louder and more persistent. The President's own Review Group on Intelligence and Communications Technology testified before the Judiciary Committee to call for an end to bulk collection, concluding that ''[t]he information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders.'' The Privacy and Civil Liberties Oversight Board also called for an end to bulk collection, concluding that the program ''lacks a viable legal foundation under Section 215.'' Technology executives, legal scholars and privacy advocates called for an end to bulk collection. These witnesses also proposed meaningful reforms to other government authorities, such as Section 702 of FISA, the pen register and trap and trace authorities under FISA, and the national security letter statutes.

Then, earlier this year, President Obama himself embraced the growing consensus that the bulk collection of phone records should not continue in its current form.

Just this week two new reports highlighted the costs of not placing reasonable limits on government surveillance, not just the significant economic cost if you don't put limits but the impact of journalistic freedom and also our right to counsel—our right to counsel—something we assume is an unalienable right, and it is, but it is being undermined.

That is why the technology industry, the privacy and civil liberties community are unified in support for this bill. It is actually now time for Congress to act.

That is why I am introducing the USA FREEDOM Act of 2014. It builds on the legislation that was passed by the House of Representatives in May, as well as the original bicameral, bipartisan legislation I introduced with Congressman JIM SENSENBRENNER 10 months ago—last October.

I continue to prefer the original version of the USA FREEDOM Act, but we are running short on time in this Congress. Since passage of the House version in May, I have been working to address concerns that the text of the House bill—though clearly intended to end bulk collection—did not do so effectively. I have worked with both Republicans and Democrats, House Members and Senators.

I spent the past several months in discussions with the intelligence community and a wide range of stakeholders, other Senators, privacy and civil liberties groups, and our U.S. technology industry.

The bill I am introducing today is the result of those hundreds of hours of negotiations and meetings.

First, and most importantly, this bill ensures that the ban on bulk collection is a real ban on bulk collection and that it is effective. It ensures the government cannot rely on section 215 of the USA PATRIOT Act—the FISA pen register and trap-and-trace device statute or the national security letter statutes—to engage in the indiscriminate collection of Americans' private records: yours, mine or anybody else's who may be watching this debate.

Under this legislation, when the government uses these authorities to collect information, it has to narrowly limit its collection based on a ''specific selection term'' that identifies the focus of the collection. ''Specific selection term'' is carefully defined. For Section 215 and the pen register statute, the definition ensures that the government must use a term that is narrowly limited to the greatest extent reasonably practicable consistent with the purpose for seeking the information. The bill specifies the term cannot be a broad geographic area, such as city or State or ZIP Code or area code, nor can it simply be a service provider. For national security letters, the government must specifically identify the target about whom it seeks information. These provisions preclude the government from seeking large swaths of information that it does not need—and that might very well include private details about the lives of law-abiding Americans.

As a backstop, the bill also mandates additional minimization procedures when the government's collection under Section 215 is likely to be overbroad. It requires the government to destroy data unrelated to its investigation within a reasonable time frame.

Second, the bill enhances transparency regarding the government's use of surveillance tools. That is one of the best checks on a runaway government. FISA and other national security laws provide law enforcement with an extraordinary amount of power. The American people have a right to know how that power is exercised.

Among other things, this bill requires the government to report to the public key information about the scope of the collection under a range of national security authorities, including the number of queries about Americans that it conducts in databases collected under Section 702. It also allows private companies more leeway to disclose the number of FISA orders and national security letters they receive.

I see the distinguished Senator from Minnesota, Mr. FRANKEN, on the floor. I thank him in particular for his leadership and helping to draft these transparency provisions.

Likewise, I thank Senator BLUMENTHAL for his work on the bill's key reforms to the FISA Court. The bill requires the FISA Court and the FISA Court of Review, in consultation with the Privacy and Civil Liberties Oversight Board, to appoint a panel of special advocates who can advance legal positions supporting individual privacy and civil liberties—in other words, it will not be just one voice that is heard, we will actually have dissenting voices—and improve judicial review.

The FISA Court would be required to appoint one of these advocates whenever it confronts a significant or novel issue of law, or it must issue a written finding that appointment of an advocate is not appropriate. The bill also requires the FISA Court to report the

number of times that it appoints or declines to appoint an advocate when confronting a novel or significant issue of law. This bill additionally provides a certification mechanism for appellate review of FISA Court decisions when the government prevails, and it provides a declassification process for significant FISA Court decisions.

Finally, this bill improves the judicial review procedures for nondisclosure orders that accompany Section 215 orders and national security letters. These have been so overused. This legislation responds to decisions by Federal courts that found these provisions violate the First Amendment.

While this bill contains significant reforms and improvements, it doesn't fix every problem, and we know there is more work to be done—in particular, with regard to Section 702 of FISA and other broad government surveillance authorities that implicate the privacy rights of Americans.

We could spend the next 20 years waiting to get 100 percent of everything we need. I would like to get most of what we need and then work on the rest.

The bill provides for public reporting on Section 702. That will help set the stage for reform, but transparency alone is not enough. I will continue to work with both Republican and Democratic Senators and other outside experts to work on these issues.

For developing the legislation, I consulted closely with the Office of the Director of National Intelligence, the NSA, the FBI, and the Department of Justice—and every single word of this bill was vetted with those agencies. I am grateful for their receptiveness to the public's concerns and for their constructive participation in this process. Together, we worked hard to ensure that this bill enacts significant and meaningful reforms to protect individual privacy, while providing the Intelligence Community with operational flexibility to safeguard this country.

The Intelligence Community will still have the ability to safeguard this country—nobody is suggesting they shouldn't, but collecting everything is the same as having nothing. That was the mistake we had before 9/11, where we had the information that could have stopped the attack on 9/11, but we failed to look at it all.

I am pleased the executive branch supports our bill. I am pleased the President agrees it should be enacted as soon as possible. But ultimately we—Senators and our colleagues in the other body—have the responsibility of the American people to do what is right and to protect the privacy of the American people. That is why we have worked hard with everybody to ensure the bill enacts meaningful reforms.

This is the most important thing to remember: We can enact this bill, get it signed into law, and it would represent the most significant reform of government surveillance authorities since Congress passed the USA PATRIOT Act 13 years ago. It is a historic opportunity. We would be derelict in our duty to this country if we passed up that opportunity.

I think if people such as Senator LEE, Senator DURBIN, Senator HELLER, Senator FRANKEN, Senator CRUZ, Senator BLUMENTHAL, Senator TOM UDALL, Senator COONS, Senator HEINRICH, Senator MARKEY, Senator HIRONO, Senator KLOBUCHAR, and Senator WHITEHOUSE have joined, this is not a partisan bill, this is not a Democratic or Republican bill, this is a good bill that protects America.

I also note the particular contributions over many years of Senator WYDEN and Senator MARK UDALL. They have worked tirelessly to protect Americans' privacy from their posts on the Intelligence Committee.

I am introducing this revised version of the USA FREEDOM Act today because we cannot afford to wait any longer to end the bulk collection of Americans' records. I am concerned that we are running out of time on the legislative calendar. Typically, my strong preference would be to take up the bill in the Judiciary Committee and mark it up. But given the need to act quickly, I am willing to forego regular order and take this bill directly to the Senate Floor.

We cannot let this opportunity go by. This is a debate about Americans' fundamental relationship with their government, about whether our government should have the power to create massive databases of information about its citizens or whether we are in control of our own government, not the other way around.

I believe we have to impose stronger limits on government surveillance powers. I am confident that most Vermonters, and most Americans, agree with me. We need to get this right, and we need to get it done without further delay.

I close with one very quick story I have used before. About the only thing I have actually saved from a newspaper that was written about me, and I liked it so much I framed it. As the distinguished Presiding Officer knows, I live on a dirt road, a place where my wife and I celebrated our honeymoon 52 years ago. The adjoining farmer has known me since I was a little kid.

The whole story in that paper goes like this: A man in an out-of-State car on a Saturday morning drives up, sees the farmer on the porch, and says:

Does Senator LEAHY live up this way?

He says: Are you a relative of his?

Well, no, I am not.

Are you a friend of his?

Well, not really.

Is he expecting you?

No.

Never heard of him.

We like our privacy.

Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

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

S. 2685

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

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 2014'' or the ''USA FREEDOM Act of 2014''.

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

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

TITLE I—FISA BUSINESS RECORDS REFORMS

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

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

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

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

Sec. 301. Limits on use of unlawfully obtained information.

TITLE IV—FOREIGN INTELLIGENCE SURVEILLANCE COURT REFORMS

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

TITLE V—NATIONAL SECURITY LETTER REFORM

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

TITLE VI—FISA TRANSPARENCY AND REPORTING REQUIREMENTS

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

TITLE VII—SUNSETS

Sec. 701. Sunsets.

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 a daily 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 call detail records—

''(I) using the specific selection term that satisfies the standard required under subsection (b)(2)(C)(ii) as the basis for production; and

''(II) using call detail records with a direct connection to such specific selection term as the basis for production of a second set of call detail records;

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

''(v) 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

''(vi) 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 authorizes 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).''.

(c) MINIMIZATION PROCEDURES.—Section 501(g)(2) (50 U.S.C. 1861(g)(2)) is amended—

(1) in subparagraph (B), by striking ''and'' at the end;

(2) by redesignating subparagraph (C) as subparagraph (D);

(3) by inserting after subparagraph (B) the following:

''(C) for orders in which the specific selection term does not specifically identify an individual, account, or personal device, procedures that prohibit the dissemination, and require the destruction within a reasonable time period (which time period shall be specified in the order), of any tangible thing or information therein that has not been determined to relate to a person who is—

''(i) a subject of an authorized investigation;

''(ii) a foreign power or a suspected agent of a foreign power;

''(iii) reasonably likely to have information about the activities of—

''(I) a subject of an authorized investigation; or

''(II) a suspected agent of a foreign power who is associated with a subject of an authorized investigation; or

''(iv) in contact with or known to—

''(I) a subject of an authorized investigation; or

''(II) a suspected agent of a foreign power who is associated with a subject of an authorized investigation,

unless the tangible thing or information therein indicates a threat of death or serious bodily harm to any person or is disseminated to another element of the intelligence community for the sole purpose of determining whether the tangible thing or information therein relates to a person who is described in clause (i), (ii), (iii), or (iv); and''; and

(4) in subparagraph (D), as so redesignated, by striking ''(A) and (B)'' and inserting ''(A), (B), and (C)''.

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) 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 2014.

''(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 2014.''.

SEC. 107. DEFINITIONS.

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

''(k) DEFINITIONS.—In this section:

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

''(2) 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 information.

''(3) SPECIFIC SELECTION TERM.—

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

''(i) means a term that specifically identifies a person, account, address, or personal device, or another specific identifier, that is used by the Government to narrowly limit the scope of tangible things sought to the greatest extent reasonably practicable, consistent with the purpose for seeking the tangible things; and

''(ii) does not include a term that does not narrowly limit the scope of the tangible things sought to the greatest extent reasonably practicable, consistent with the purpose for seeking the tangible things, such as—

''(I) a term based on a broad geographic region, including a city, State, zip code, or area code, when not used as part of a specific identifier as described in clause (i); or

''(II) a term identifying 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 of production.

''(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. 108. 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 December 31, 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. 109. 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) 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. 110. 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)—

(A) by striking ''a certification by the applicant'' and inserting ''a statement of the facts and circumstances relied upon by the applicant to justify the belief of the applicant''; and

(B) by striking the period 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 installation or 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) means a term that specifically identifies a person, account, address, or personal device, or another specific identifier, that is used by the Government to narrowly limit the scope of information sought to the greatest extent reasonably practicable, consistent with the purpose for the installation or use of the pen register or trap and trace device; and

''(ii) does not include a term that does not narrowly limit the scope of information sought to the greatest extent reasonably practicable, consistent with the purpose for the installation or use of the pen register or trap and trace device, such as—

''(I) a term based on a broad geographic region, including a city, State, zip code, or area code, when not used as part of a specific identifier as described in clause (i); or

''(II) a term identifying an electronic communication service provider (as 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 installation or use of the pen register or trap and trace device.

''(B) For purposes of subparagraph (A), the term 'address' means a physical address or electronic address, such as an electronic mail address, temporarily assigned network address, or Internet protocol address.''.

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 shall be construed to limit 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.

''(3) COMPLIANCE ASSESSMENT.—At or before the end of the period of time for which the installation and use of a pen register or trap and trace device is approved under an order or an extension under this section, the judge may assess compliance with the privacy procedures required by this subsection by reviewing the circumstances under which information concerning United States persons was collected, retained, or disseminated.''.

(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 shall establish 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 subsection:

''(i) AMICUS CURIAE.—

''(1) APPOINTMENT OF SPECIAL ADVOCATES.—In consultation with the Privacy and Civil Liberties Oversight Board, 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 appoint not fewer than 5 attorneys to serve as special advocates, who shall serve pursuant to rules the presiding judges may establish. Such individuals shall be persons who possess expertise in privacy and civil liberties, intelligence collection, telecommunications, or any other relevant area of expertise and who are determined to be eligible for access to classified information necessary to participate in matters before the courts.

''(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 designate a special advocate to serve as amicus curiae to assist such court in the consideration of any certification pursuant to subsection (j) or 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 written finding that such appointment is not appropriate; and

''(B) may designate or allow an individual or organization to serve as amicus curiae or to provide technical expertise in any other instance as such court deems appropriate.

''(3) RULE OF CONSTRUCTION.—An application for an order or review shall be considered to present a novel or significant interpretation of the law if such application involves application of settled law to novel technologies or circumstances, or any other novel or significant construction or interpretation of any provision of law or of the Constitution of the United States, including any novel and significant interpretation of the term 'specific selection term'.

''(4) DUTIES.—

''(A) IN GENERAL.—If a court established under subsection (a) or (b) designates a special advocate to participate as an amicus curiae in a proceeding, the special advocate—

''(i) shall advocate, as appropriate, in support of legal interpretations that advance individual privacy and civil liberties;

''(ii) shall have access to all relevant legal precedent, and any application, certification, petition, motion, or such other materials as are relevant to the duties of the special advocate;

''(iii) may consult with any other special advocates regarding information relevant to any assigned case, including sharing relevant materials; and

''(iv) may request that the court appoint technical and subject matter experts, not employed by the Government, to be available to assist the special advocate in performing the duties of the special advocate.

''(B) BRIEFINGS OR ACCESS TO MATERIALS.—The Attorney General shall periodically brief or provide relevant materials to special advocates regarding constructions and interpretations of this Act and legal, technological and other issues related to actions authorized by this Act.

''(C) ACCESS TO CLASSIFIED INFORMATION.—

''(i) IN GENERAL.—A special advocate, experts appointed to assist a special advocate, or any other amicus or technical expert 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.

''(ii) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to require the Government to provide information to a special advocate, other amicus, or technical expert that is privileged from disclosure.

''(5) NOTIFICATION.—The presiding judges of the courts established under subsections (a) and (b) shall notify the Attorney General of each exercise of the authority to appoint an individual to serve as 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 for an individual appointed to serve as a special advocate under paragraph (1) in a manner that is not inconsistent with this subsection.

''(j) REVIEW OF FISA COURT DECISIONS.—After issuing an order, a court established under subsection (a) shall certify for review to the court established under subsection (b) any question of law 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 paragraph, 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 any decision issued by the court of review established under subsection (b) approving, in whole or in part, an application by the Government under this Act, such court may certify at any time, including after a decision, a question of law to be reviewed by the Supreme Court of the United States.

''(2) SPECIAL ADVOCATE BRIEFING.—Upon certification of an application under paragraph (1), the court of review established under subsection (b) may designate a special advocate to provide briefing as prescribed by the Supreme Court.

''(3) REVIEW.—The Supreme Court may review any question of law certified under paragraph (1) by the court of review established under subsection (b) in the same manner as the Supreme Court reviews questions certified under section 1254(2) of title 28, United States Code.

''(l) PAYMENT FOR SERVICE AS SPECIAL ADVOCATE.—A special advocate designated in a proceeding pursuant to subsection (i)(2)(A) of this section may seek, at the conclusion of the proceeding in which the special advocate was designated, compensation for services provided pursuant to the designation. A special advocate seeking compensation shall be compensated in an amount reflecting fair compensation for the services provided, as determined by the court designating the special advocate and approved by the presiding judges of the courts established under subsections (a) and (b).

''(m) APPROPRIATIONS.—There are authorized to be appropriated to the United States courts such sums as may be necessary to carry out the provisions of this section. When so specified in appropriation acts, such appropriations shall remain available until expended. Payments from such appropriations shall be made under the supervision of the Director of the Administrative Office of the United States Courts.''.

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 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 law, which shall include, to the extent consistent with national security, each legal question addressed by the decision and how such question was resolved, in general terms the context in which the matter arises, and a description of the 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.

''(3) TERMINATION.—

''(A) IN GENERAL.—In the case of any request under subsection (b) for which a recipient has submitted a notification to the Government under section 3511(b)(1)(A) or filed a petition for judicial review under subsection (d)—

''(i) an appropriate official of the Federal Bureau of Investigation shall, until termination of the nondisclosure requirement, review the facts supporting a nondisclosure requirement annually and upon closure of the investigation; and

''(ii) if, upon a review under clause (i), the facts no longer support the nondisclosure requirement, an appropriate official of the Federal Bureau of Investigation shall promptly notify the wire or electronic service provider, or officer, employee, or agent thereof, subject to the nondisclosure requirement, and the court as appropriate, that the nondisclosure requirement is no longer in effect.

''(B) CLOSURE OF INVESTIGATION.—Upon closure of the investigation—

''(i) the Federal Bureau of Investigation may petition the court before which a notification or petition for judicial review under subsection (d) has been filed for a determination that disclosure may result in the harm described in clause (i), (ii), (iii), or (iv) of paragraph (1)(B), if it notifies the recipient of such petition;

''(ii) the court shall review such a petition pursuant to the procedures under section 3511; and

''(iii) if the court determines that there is reason to believe that disclosure may result in the harm described in clause (i), (ii), (iii), or (iv) of paragraph (1)(B), the Federal Bureau of Investigation shall no longer be required to conduct the annual review of the facts supporting the nondisclosure requirement under subparagraph (A).''.

(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.

''(3) TERMINATION.—

''(A) IN GENERAL.—In the case of any request under subsection (a) for which a recipient has submitted a notification to the Government under section 3511(b)(1)(A) of title 18, United States Code, or filed a petition for judicial review under subsection (d)—

''(i) an appropriate official of the Federal Bureau of Investigation shall, until termination of the nondisclosure requirement, review the facts supporting a nondisclosure requirement annually and upon closure of the investigation; and

''(ii) if, upon a review under clause (i), the facts no longer support the nondisclosure requirement, an appropriate official of the Federal Bureau of Investigation shall promptly notify the financial institution, or officer, employee, or agent thereof, subject to the nondisclosure requirement, and the court as appropriate, that the nondisclosure requirement is no longer in effect.

''(B) CLOSURE OF INVESTIGATION.—Upon closure of the investigation—

''(i) the Federal Bureau of Investigation may petition the court before which a notification or petition for judicial review under subsection (d) has been filed for a determination that disclosure may result in the harm described in clause (i), (ii), (iii), or (iv) of paragraph (1)(B), if it notifies the recipient of such petition;

''(ii) the court shall review such a petition pursuant to the procedures under section 3511 of title 18, United States Code; and

''(iii) if the court determines that there is reason to believe that disclosure may result in the harm described in clause (i), (ii), (iii), or (iv) of paragraph (1)(B), the Federal Bureau of Investigation shall no longer be required to conduct the annual review of the facts supporting the nondisclosure requirement under subparagraph (A).''.

(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.

''(3) TERMINATION.—

''(A) IN GENERAL.—In the case of any request under subsection (a) or (b) or order under subsection (c) for which a recipient has submitted a notification to the Government under section 3511(b)(1)(A) of title 18, United States Code, or filed a petition for judicial review under subsection (e)—

''(i) an appropriate official of the Federal Bureau of Investigation shall, until termination of the nondisclosure requirement, review the facts supporting a nondisclosure requirement annually and upon closure of the investigation; and

''(ii) if, upon a review under clause (i), the facts no longer support the nondisclosure requirement, an appropriate official of the Federal Bureau of Investigation shall promptly notify the consumer reporting agency, or officer, employee, or agent thereof, subject to the nondisclosure requirement, and the court as appropriate, that the nondisclosure requirement is no longer in effect.

''(B) CLOSURE OF INVESTIGATION.—Upon closure of the investigation—

''(i) the Federal Bureau of Investigation may petition the court before which a notification or petition for judicial review under subsection (e) has been filed for a determination that disclosure may result in the harm described in clause (i), (ii), (iii), or (iv) of paragraph (1)(B), if it notifies the recipient of such petition;

''(ii) the court shall review such a petition pursuant to the procedures under section 3511 of title 18, United States Code; and

''(iii) if the court determines that there is reason to believe that disclosure may result in the harm described in clause (i), (ii), (iii), or (iv) of paragraph (1)(B), the Federal Bureau of Investigation shall no longer be required to conduct the annual review of the facts supporting the nondisclosure requirement under subparagraph (A).''.

(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.

''(3) TERMINATION.—

''(A) IN GENERAL.—In the case of any request under subsection (a) for which a recipient has submitted a notification to the Government under section 3511(b)(1)(A) of title 18, United States Code, or filed a petition for judicial review under subsection (d)—

''(i) an appropriate official of the agency described in subsection (a) shall, until termination of the nondisclosure requirement, review the facts supporting a nondisclosure requirement annually and upon closure of the investigation; and

''(ii) if, upon a review under clause (i), the facts no longer support the nondisclosure requirement, an appropriate official of the agency described in subsection (a) shall promptly notify the consumer reporting agency, or officer, employee, or agent thereof, subject to the nondisclosure requirement, and the court as appropriate, that the nondisclosure requirement is no longer in effect.

''(B) CLOSURE OF INVESTIGATION.—Upon closure of the investigation—

''(i) the agency described in subsection (a) may petition the court before which a notification or petition for judicial review under subsection (d) has been filed for a determination that disclosure may result in the harm described in clause (i), (ii), (iii), or (iv) of paragraph (1)(B), if it notifies the recipient of such petition;

''(ii) the court shall review such a petition pursuant to the procedures under section 3511 of title 18, United States Code; and

''(iii) if the court determines that there is reason to believe that disclosure may result in the harm described in clause (i), (ii), (iii), or (iv) of paragraph (1)(B), the agency described in subsection (1) shall no longer be required to conduct the annual review of the facts supporting the nondisclosure requirement under subparagraph (A).''.

(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.

''(3) TERMINATION.—

''(A) IN GENERAL.—In the case of any request for which a recipient has submitted a notification to the Government under section 3511(b)(1)(A) of title 18, United States Code, or filed a petition for judicial review under subsection (c)—

''(i) an appropriate official of the authorized investigative agency making the request under subsection (a) shall, until termination of the nondisclosure requirement, review the facts supporting a nondisclosure requirement annually and upon closure of the investigation; and

''(ii) if, upon a review under clause (i), the facts no longer support the nondisclosure requirement, an appropriate official of the authorized investigative agency making the request under subsection (a) shall promptly notify the recipient of the request, or officer, employee, or agent thereof, subject to the nondisclosure requirement, and the court as appropriate, that the nondisclosure requirement is no longer in effect.

''(B) CLOSURE OF INVESTIGATION.—Upon closure of the investigation—

''(i) the authorized investigative agency making the request under subsection (a) may petition the court before which a notification or petition for judicial review under subsection (c) has been filed for a determination that disclosure may result in the harm described in clause (i), (ii), (iii), or (iv) of paragraph (1)(B), if it notifies the recipient of such petition;

''(ii) the court shall review such a petition pursuant to the procedures under section 3511 of title 18, United States Code; and

''(iii) if the court determines that there is reason to believe that disclosure may result in the harm described in clause (i), (ii), (iii),

or (iv) of paragraph (1)(B), the authorized investigative agency shall no longer be required to conduct the annual review of the facts supporting the nondisclosure requirement under subparagraph (A).''.

(f) 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.

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;''.

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.—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, made publicly available on an Internet Web site, that includes—

''(1) the number of applications or certifications for orders submitted under each of sections 105, 304, 402, 501, 702, 703, and 704;

''(2) the number of orders entered under each of those sections;

''(3) the number of orders modified under each of those sections;

''(4) the number of orders denied under each of those sections;

''(5) 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

''(6) the number of written findings issued under section 103(i) that such appointment is not appropriate and the text of any such written findings.

''(b) MANDATORY REPORTING BY DIRECTOR OF NATIONAL INTELLIGENCE.—

''(1) IN GENERAL.—Except as provided in subsection (e), 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—

''(A) 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;

''(B) the total number of orders issued pursuant to section 702 and a good faith estimate of—

''(i) the number of targets of such orders;

''(ii) the number of individuals whose communications were collected pursuant to such orders;

''(iii) the number of individuals whose communications were collected pursuant to such orders who are reasonably believed to have been located in the United States at the time of collection;

''(iv) the number of search terms that included information concerning a United States person that were used to query any database of the contents of electronic communications or wire communications obtained through the use of an order issued pursuant to section 702; and

''(v) the number of search queries initiated by an officer, employee, or agent of the United States whose search terms included information concerning a United States person in any database of noncontents information relating to electronic communications or wire communications that were obtained through the use of an order issued pursuant to section 702;

''(C) the total number of orders issued pursuant to title IV and a good faith estimate of—

''(i) the number of targets of such orders;

''(ii) the number of individuals whose communications were collected pursuant to such orders; and

''(iii) the number of individuals whose communications were collected pursuant to such orders who are reasonably believed to have been located in the United States at the time of collection;

''(D) the total number of orders issued pursuant to applications made under section 501(b)(2)(B) and a good faith estimate of—

''(i) the number of targets of such orders;

''(ii) the number of individuals whose communications were collected pursuant to such orders; and

''(iii) the number of individuals whose communications were collected pursuant to such orders who are reasonably believed to have been located in the United States at the time of collection;

''(E) the total number of orders issued pursuant to applications made under section 501(b)(2)(C) and a good faith estimate of—

''(i) the number of targets of such orders;

''(ii) the number of individuals whose communications were collected pursuant to such orders;

''(iii) the number of individuals whose communications were collected pursuant to such orders who are reasonably believed to have been located in the United States at the time of collection; and

''(iv) 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

''(F) the total number of national security letters issued and the number of requests for information contained within such national security letters.

''(2) BASIS FOR REASONABLE BELIEF INDIVIDUAL IS LOCATED IN UNITED STATES.—A phone number registered in the United States may provide the basis for a reasonable belief that the individual using the phone number is located in the United States at the time of collection.

''(c) DISCRETIONARY REPORTING BY DIRECTOR OF NATIONAL INTELLIGENCE.—The Director of National Intelligence may annually make publicly available on an Internet Web site a report that identifies, for the preceding 12-month period—

''(1) a good faith estimate of the number of individuals whose communications were collected pursuant to orders issued pursuant to titles I and III and sections 703 and 704 reasonably believed to have been located in the United States at the time of collection whose information was reviewed or accessed by an officer, employee, or agent of the United States;

''(2) a good faith estimate of the number of individuals whose communications were collected pursuant to orders issued pursuant to section 702 reasonably believed to have been located in the United States at the time of collection whose information was reviewed or accessed by an officer, employee, or agent of the United States;

''(3) a good faith estimate of the number of individuals whose communications were collected pursuant to orders issued pursuant to title IV reasonably believed to have been located in the United States at the time of collection whose information was reviewed or accessed by an officer, employee, or agent of the United States;

''(4) a good faith estimate of the number of individuals whose communications were collected pursuant to orders issued pursuant to applications made under section 501(b)(2)(B) reasonably believed to have been located in the United States at the time of collection whose information was reviewed or accessed by an officer, employee, or agent of the United States; and

''(5) a good faith estimate of the number of individuals whose communications were collected pursuant to orders issued pursuant to applications made under section 501(b)(2)(C) reasonably believed to have been located in the United States at the time of collection whose information was reviewed or accessed by an officer, employee, or agent of the United States.

''(d) TIMING.—The annual reports required by subsections (a) and (b) and permitted by subsection (c) shall be made publicly available during April of each year and include information relating to the previous year.

''(e) EXCEPTIONS.—

''(1) REPORTING BY UNIQUE IDENTIFIER.—If it is not practicable to report the good faith estimates required by subsection (b) and permitted by subsection (c) in terms of individuals, the good faith estimates may be counted in terms of unique identifiers, including names, account names or numbers, addresses, or telephone or instrument numbers.

''(2) STATEMENT OF NUMERICAL RANGE.—If a good faith estimate required to be reported under clauses (ii) or (iii) of each of subparagraphs (B), (C), (D), and (E) of paragraph (1) of subsection (b) or permitted to be reported in subsection (c), is fewer than 500, it shall exclusively be expressed as a numerical range of 'fewer than 500' and shall not be expressed as an individual number.

''(3) FEDERAL BUREAU OF INVESTIGATION.—Subparagraphs (B)(iv), (B)(v), (D)(iii), (E)(iii), and (E)(iv) of paragraph (1) of subsection (b) shall not apply to information or records held by, or queries conducted by, the Federal Bureau of Investigation.

''(4) CERTIFICATION.—

''(A) IN GENERAL.—If the Director of National Intelligence concludes that a good faith estimate required to be reported under subparagraph (B)(iii) or (C)(iii) of paragraph (1) of subsection (b) cannot be determined accurately, including through the use of statistical sampling, the Director shall—

''(i) certify that conclusion in writing 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; and

''(ii) make such certification publicly available on an Internet Web site.

''(B) CONTENT.—

''(i) IN GENERAL.—The certification described in subparagraph (A) shall state with specificity any operational, national security, or other reasons why the Director of National Intelligence has reached the conclusion described in subparagraph (A).

''(ii) GOOD FAITH ESTIMATES OF CERTAIN INDIVIDUALS WHOSE COMMUNICATIONS WERE COLLECTED UNDER ORDERS ISSUED UNDER SECTION 702.—A certification described in subparagraph (A) relating to a good faith estimate required to be reported under subsection (b)(1)(B)(iii) may include the information annually reported pursuant to section 702(l)(3)(A).

''(iii) GOOD FAITH ESTIMATES OF CERTAIN INDIVIDUALS WHOSE COMMUNICATIONS WERE COLLECTED UNDER ORDERS ISSUED UNDER TITLE IV.—If the Director of National Intelligence determines that a good faith estimate required to be reported under subsection (b)(1)(C)(iii) cannot be determined accurately as that estimate pertains to electronic communications, but can be determined accurately for wire communications, the Director shall make the certification described in subparagraph (A) with respect to electronic communications and shall also report the good faith estimate with respect to wire communications.

''(C) FORM.—A certification described in subparagraph (A) shall be prepared in unclassified form, but may contain a classified annex.

''(D) 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.

''(f) CONSTRUCTION.—Nothing in this section affects the lawfulness or unlawfulness of any government surveillance activities described herein.

''(g) 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) INDIVIDUAL WHOSE COMMUNICATIONS WERE COLLECTED.—The term 'individual whose communications were collected' means any individual—

''(A) who was a party to an electronic communication or a wire communication the contents or noncontents of which was collected; or

''(B)(i) who was a subscriber or customer of an electronic communication service or remote computing service; and

''(ii) whose records, as described in subparagraph (A), (B), (D), (E), or (F) of section 2703(c)(2) of title 18, United States Code, were collected.

''(4) 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)).

''(5) 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))).

''(6) 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 ''concerning different United States persons''; 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 1 of the following structures:

''(1) A semiannual report that aggregates the number of orders or national security letters with which the person was required to comply in the following separate categories:

''(A) The number of national security letters received, reported in bands of 1000 starting with 0–999.

''(B) The number of customer accounts affected by national security letters, reported in bands of 1000 starting with 0–999.

''(C) The number of orders under this Act for contents, reported in bands of 1000 starting with 0–999.

''(D) With respect to contents orders under this Act, in bands of 1000 starting with 0–999, the number of customer selectors targeted under such orders.

''(E) The number of orders under this Act for noncontents, reported in bands of 1000 starting with 0–999.

''(F) With respect to noncontents orders under this Act, in bands of 1000 starting with 0–999, the number of customer selectors targeted under orders under—

''(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 in the following separate categories:

''(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 0–249 and thereafter in bands of 250.

''(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 0–249 and thereafter in bands of 250.

''(3) A semiannual report that aggregates the number of orders or national security letters with which the person was required to comply in the following separate categories:

''(A) The number of national security letters received, reported in bands of 500 starting with 0–499.

''(B) The number of customer accounts affected by national security letters, reported in bands of 500 starting with 0–499.

''(C) The number of orders under this Act for contents, reported in bands of 500 starting with 0–499.

''(D) The number of customer selectors targeted under such orders, reported in bands of 500 starting with 0–499.

''(E) The number of orders under this Act for noncontents, reported in bands of 500 starting with 0–499.

''(F) The number of customer selectors targeted under such orders, reported in bands of 500 starting with 0–499.

''(4) An annual report that aggregates the number of orders, directives, and national security letters the person was required to comply with in the following separate categories:

''(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 0–100 and thereafter in bands of 100.

''(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 0–100 and thereafter in bands of 100.

''(b) PERIOD OF TIME COVERED BY REPORTS.—

''(1) A report described in paragraph (1) or (3) of subsection (a)—

''(A) may be published every 180 days;

''(B) subject to subparagraph (C), shall include—

''(i) with respect to information relating to national security letters, information relating to the previous 180 days; and

''(ii) with respect to information relating to authorities under this Act, except as provided in subparagraph (C), information relating to the time period—

''(I) ending on the date that is not less than 180 days before the date on which the information is publicly reported; and

''(II) beginning on the date that is 180 days before the date described in subclause (I); and

''(C) for a person that has received an order or directive under this Act with respect to a platform, product, or service for which a person did not previously receive such an order or directive (not including an enhancement to or iteration of an existing publicly available platform, product, or service)—

''(i) 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; and

''(ii) for a report published on or after the date on which the 540-day waiting period expires, shall include information relating to such new order or directive reported pursuant to subparagraph (B)(ii).

''(2) A report described in paragraph (2) of subsection (a) may be published every 180 days and shall include information relating to the previous 180 days.

''(3) A report described in paragraph (4) of subsection (a) may be published annually and shall include information relating to the time period—

''(A) ending on the date that is not less than 1 year before the date on which the information is publicly reported; and

''(B) beginning on the date that is 1 year before the date described in subparagraph (A).

''(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—SUNSETS

SEC. 701. 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 31, 2017''.

(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 31, 2017''.

Mr. LEE. First, I thank my distinguished colleague, the senior Senator from Vermont, for his leadership on this issue. I am pleased to join him as a cosponsor of this legislation. As the lead cosponsor of this bill, I attest to the fact that this is an issue that is neither Republican nor Democratic, it is neither liberal nor conservative, it is simply American.

It is a fundamental concept of liberty that we have to control the government. The government and the immense power of government has expanded over time with advances in technology. Our country certainly has changed to an enormous degree over the centuries since James Madison penned our Bill of Rights. But the protection of liberty afforded by the Fourth Amendment has only become more important, not less important, as the government's ability to collect information has advanced.

This legislation, which has broad-based bipartisan support, is absolutely necessary. It can be implemented in a way that will still allow the government to protect us. It will also protect us from the risk of overreach by the government.

We have to remember it is not just the government that we have in place today, even if we assume, for purposes of this discussion, that everyone who works for the government, every government agent who participates in the collection of this information is doing what is right. We can't always assume that will be the case in the future.

I see my time has expired. I once again thank my colleague, the senior Senator from Vermont, Mr. LEAHY, for his sponsorship of this legislation. I urge my colleagues to join us in this effort.

Mr. FRANKEN. Mr. President, I rise to talk about the transparency provisions in the USA FREEDOM Act. I am a proud cosponsor of Chairman LEAHY's bill, and I am particularly proud to have written the key transparency provisions with my friend Senator DEAN HELLER of Nevada.

Senator LEE is right. This is not a Republican bill or a Democratic bill. This isn't a Republican issue or a Democratic issue. I thank Senator LEE for his leadership. Of course, we are all indebted to Senator LEAHY for his leadership on this issue.

Because of time constraints, I am not going to be able to give the speech I wanted to, so I will try to ask for time for tomorrow. I know today's floor is very busy.

I wish to say it is very important that there is enough transparency in our NSA surveillance that Americans can judge for themselves if we are striking the right balance between national security and our civil liberties.

Mr. HELLER. Mr. President, today my colleague Senator LEAHY, the chairman of the Judiciary Committee, introduced legislation that would amend the PATRIOT Act. This new legislation reflects a bicameral and bipartisan compromise that ends the bulk data collection practices currently being used. It also gives our intelligence officials specific rules to follow so they can keep the operational capabilities necessary to protect the United States from a terrorist attack without compromising the Fourth Amendment to the Constitution. I thank Senator LEAHY for his work, and I am grateful for his partnership.

This important step is necessary for restoring Americans' privacy rights which were taken by a well-intended but overreaching Federal Government in the wake of the 9/11 terrorist attacks.

The expanded authority given to the National Security Agency through executive action and the PATRIOT Act was intended to prevent another attack on America. While I was not a Member of Congress on 9/11, I shared the horror all Nevadans felt watching the murder of thousands of innocent Americans, and the profound sadness as buildings in New York and Washington, DC, sat smoldering. I understand as well as anyone here the reason behind the actions our Nation's leaders took to ensure that another attack on America never materialized, and why our leaders felt that no limits should be imposed. No matter what the cost, Americans had to be protected against another attack.

Viewing the situation from that lens, it is easy to understand how the Fourth Amendment was brushed aside as the Senate expanded law enforcement surveillance capabilities with just one dissenting vote.

The Federal Bureau of Investigation then used section 215 of the PATRIOT Act to expand the scope of surveillance far beyond even what some of the authors believed they were authorizing. The FBI argued that section 215 provided authority to collect phone data of law-abiding citizens without their knowledge. Specifically, they could use the business records provision to force phone companies to turn over millions of telephone calls when there is a reasonable ground or relevance to believe that the information sought is relevant to an authorized investigation of international terrorism.

As a result, we now have a bulk collection program in existence where telephone companies hand over millions of records to the NSA as part of a massive pre-collection database.

As someone who voted against the PATRIOT Act time and time again, I believe such data collection practices are a massive intrusion of our privacy, which is why I partnered with the senior Senator from Vermont to end these programs. Our legislation tightens the definitions of ''specific selection term'' for section 215 of the PATRIOT Act and FISA pen register trap-and-trace devices so that the information requested is limited to specifically identifying a person, account, address, or a personal device.

With this legislation, bulk collection will be eliminated and the records will stay with the telephone companies. The massive information grabs from the Federal Government based on geography or email service will no longer be permissible. And of the information that is collected, the legislation imposes new restrictions on its use and retention. These reforms will help shift the balance of privacy away from the Federal Government and back to the American people.

I am proud that this bill also includes the Franken-Heller Surveillance

Transparency Act of 2013. I was pleased to join Senator FRANKEN on this legislation because, at the very least, Americans deserve to know the number of people whose information is housed by the NSA. For the first time in American history, the government is forced to disclose to the American people roughly how many of them have had their communications collected.

Our provision calls for reports by the Director of National Intelligence detailing the requests for information authorized under the PATRIOT Act and the FISA Amendments Act. The reports would specify the total number of people whose information has been collected under these programs and how many people living in the United States have had their information collected. They would also permit the intelligence community to report on how many Americans actually had their information looked at by the NSA or any other intelligence agencies.

Furthermore, these provisions would allow telephone and Internet companies to tell consumers basic information regarding FISA court orders they receive and the number of users whose information is turned over.

The principles outlined in this bill to increase transparency for Americans and private companies would clear up a tremendous amount of confusion that exists within the programs. And our private companies need the added disclosure. The Information Technology & Innovation Foundation estimates that American cloud computing companies could lose $22 billion to $35 billion in the next 3 years because of concerns about their involvement with surveillance programs. The analytics firm Forrester put potential losses much higher, at $180 billion.

I want to be clear: I share the concerns of all Americans that we must protect ourselves against threats to the homeland. I believe terrorism is very real and the United States is the target of those looking to undermine the freedoms we hold as the core of our national identity. If the bulk collection programs in existence were bearing so much information to protect the homeland, it would change my opinion on the need for the USA Freedom Act. However, the bulk collection program has simply not provided the tangible results that justify a privacy intrusion of this level. We know this because on October 2, 2013, the chairman of the Senate Judiciary Committee, Senator LEAHY, asked NSA Director Keith Alexander the following question:

> At our last hearing, deputy director Inglis stated that there's only really one example of a case where, but for the use of Section 215 bulk phone records collection, terrorist activity was stopped. Was Mr. Inglis right?

To which Director Alexander responded:

> He's right. I believe he said two, Chairman.

Congress has authorized the collection of millions of law-abiding citizens' telephone metadata for years and it has only solved two ongoing FBI investigations. Of those two investigations, the NSA has publicly identified one. In fact, that case could have easily been handled by obtaining a warrant and going to the telephone company. It is the case of an individual in San Diego who was convicted of sending $8,500 to Somalia in support of al-Shabaab, the terrorist organization claiming responsibility for the Kenyan mall attack. The American phone records allowed the NSA to determine that a U.S. phone was used to contact an individual associated with this terrorist organization. I am appreciative that the NSA was able to apprehend this individual, but it does not provide overwhelming evidence that this program is necessary. The Obama administration has come to the same conclusion and so has the intelligence community.

The operational capabilities the intelligence community relies on to conduct their mission to keep us safe will not be impacted by the USA FREEDOM Act. If it were, the Intelligence Community and the administration would not have brokered this compromise legislation. Ending the bulk collection programs and giving Americans more transparency so they can determine for themselves whether they believe these programs should exist is an obligation we have to all of our constituents.

We have a bill introduced today that would give our law enforcement authorities the tools they need to keep us safe and also stay true to the Fourth Amendment. I encourage my colleagues to support these important reforms and I hope it can quickly be considered by this Chamber.

SUBMITTED RESOLUTIONS

SENATE RESOLUTION 526—SUPPORTING ISRAEL'S RIGHT TO DEFEND ITSELF AGAINST HAMAS, AND FOR OTHER PURPOSES

Mr. REID (for himself, Mr. MCCONNELL, Mr. MENENDEZ, Mr. CORKER, Mr. CARDIN, and Mr. GRAHAM) submitted the following resolution; which was considered and agreed to.:

S. RES. 526

Whereas Hamas, an organization designated as a Foreign Terrorist Organization by the United States Department of State since 1997, has fired over 2,500 rockets indiscriminately from Gaza into Israel;

Whereas Israel has a right to defend itself from Hamas's constant barrage of rockets and to destroy the matrix of tunnels Hamas uses to smuggle weapons and Hamas fighters into Israel to carry out terrorist attacks;

Whereas the Government of Israel has taken significant steps to protect civilians in Gaza, including dropping leaflets in Gaza neighborhoods in advance of Israeli military attacks, calling Palestinians on the phone urging them to evacuate certain areas before the military strikes targets, and issuing warnings to civilians in advance of firing on buildings;

Whereas Israel's attacks have focused on terrorist targets such as Hamas's munitions storage sites, areas sheltering Hamas's rocket systems, Hamas's weapons manufacturing sites, the homes of militant leaders, and on the vast labyrinth of tunnels Hamas's fighters use to penetrate Israel's territory and attack Israelis;

Whereas Hamas uses rockets to indiscriminately target civilians in Israel;

Whereas Israel has accepted and implemented numerous ceasefire agreements that Hamas has rejected;

Whereas Hamas continued to fire rockets into Israel during a 24-hour truce that Hamas had itself proposed;

Whereas Israel embraced the Egyptian-proposed ceasefire agreement, which Hamas resoundingly rejected on July 27, 2014;

Whereas Hamas intentionally uses civilians as human shields;

Whereas Hamas refuses to recognize Israel's right to exist;

Whereas Israel's Iron Dome has protected Israel's civilian population from the over 2,500 rockets that Hamas has indiscriminately fired into Israel since July 7, 2014;

Whereas, without Iron Dome's ability to intercept and destroy Hamas's missiles, Israeli neighborhoods would have been significantly damaged and Israeli casualties would have been much higher;

Whereas the United Nations Human Rights Council voted to accept a biased resolution establishing a Commission of Inquiry to determine if Israel violated human rights and humanitarian law during the ongoing conflict with Gaza; and

Whereas the United Nations Human Rights Council resolution makes no mention of investigating Hamas's indiscriminate rocket attacks against Israel, nor Hamas's policy of using Palestinian civilians as human shields: Now, therefore, be it

Resolved, That the Senate—

(1) laments all loss of innocent civilian life;

(2) condemns the United Nations Human Rights Council's resolution on July 23, 2014, which calls for yet another prejudged investigation of Israel while making no mention of Hamas's continued assault against Israel, and also calls for an investigation into potential human rights violations by Israel in the current Gaza conflict without mentioning Hamas's assault against innocent civilians and its use of civilian shields;

(3) supports Israel's right to defend itself against Hamas's unrelenting and indiscriminate rocket assault into Israel and Israel's right to destroy Hamas's elaborate tunnel system into Israel's territory;

(4) condemns Hamas's terrorist actions and use of civilians as human shields;

(5) supports United States mediation efforts for a durable ceasefire agreement that immediately ends Hamas's rocket assault and leads to the demilitarization of Gaza; and

(6) supports additional funding the Government of Israel needs to replenish Iron Dome missiles and enhance Israel's defensive capabilities.