113TH CONGRESS | REPORT
1st Session | SENATE | 113-

FISA IMPROVEMENTS ACT OF 2013

NOVEMBER 12, 2013 – Ordered to be printed

Mrs. FEINSTEIN, from the Select Committee on Intelligence, submitted the following

R E P O R T

together with

ADDITIONAL VIEWS

To accompany S. 1631

The Select Committee on Intelligence, having considered an original bill (S. 1631) to make improvements to the Foreign Intelligence Surveillance Act of 1978, as amended (FISA), and for other purposes, reports favorably thereon and recommends that the bill do pass.

BACKGROUND AND NEED FOR LEGISLATION

The Committee, since its inception in 1976, has considered oversight of the Executive branch's use of electronic surveillance for foreign intelligence purposes to be one of its most important responsibilities. Since 2006, a central focus of that oversight has included the Executive branch's use of Section 215 of the USA PATRIOT Act (Section 501 of FISA) to conduct bulk collection of "call data records" that contain metadata concerning domestic and international telephone calls, including the numbers dialed, as well as the time, date, and duration of the calls, but not the content of the calls.

The Committee has not been alone in its oversight of this telephone metadata program. The Senate Judiciary Committee, as well as the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives, also has received regular reports and briefings on the program. In addition, information concerning the bulk telephone metadata program has been made available to every member of the Senate prior to the reauthorization of Section 215, most recently in 2011.

As the Committee has reauthorized the business records provision in the past, it has found the program to be an effective counterterrorism tool and one that was determined by the Department of Justice in two Administrations and by at least fifteen different judges serving on

the Foreign Intelligence Surveillance Court (FISC) to be lawful. In hearings and in mark-ups, the Committee has discussed the program and determined on a strong bipartisan basis that the legal authorities supporting the program should be reauthorized.

Through the Committee's oversight of the program, the Committee has been made aware of instances of inadvertent non-compliance with the law or other policies and procedures governing the telephone metadata program. Where such incidents have arisen, they have been the result of human error or technical defect—not intentional abuse—and have been promptly reported and remedied. Further, the Committee has performed extensive oversight of such incidents to help ensure necessary measures were taken to correct the deficiencies that gave rise to the compliance incidents. It remains the case that, through seven years of oversight of this metadata program under Section 215, the Committee has not identified a single case in which a government official engaged in a willful effort to circumvent or violate Section 215 in the conduct of the bulk telephone metadata program.

Similarly, the Committee has conducted oversight of the implementation of Section 702 of FISA as established in 2008 by the FISA Amendments Act. The Committee has found that authority, which allows for the collection of the electronic communications of non-U.S. Persons outside the United States under procedures approved annually by the FISC, to be extremely effective in producing foreign intelligence concerning terrorists, weapons proliferators, and other adversaries. This provision has been the subject of significant noncompliance issues in the past, but as with the business records metadata program, those issues have been uniformly unintentional, self-identified, and reported to the Court and to Congress.

Until earlier this year, key aspects of both the business records program and the Section 702 collection were highly classified. Following the unprecedented leaks of classified information, primarily of information relating to the National Security Agency (NSA), by former NSA contractor Edward Snowden, most of both programs' secrets have been declassified by the Director of National Intelligence (DNI). The nature of the leaks has caused public concern over the use of these authorities, notwithstanding the care demonstrated by the NSA to abide by the law and to protect U.S. Persons' private information. This has led to a series of Committee hearings and discussions over ways to add additional privacy protections and transparency measures to FISA operations, while preserving the operational effectiveness and flexibility of the programs, resulting in this legislation. The Committee remains of the view that these programs are effective, lawful, and subject to significant oversight and review within the Intelligence Community and by the Department of Justice, the FISC, and the Congress.

This legislation includes a series of measures that make improvements to FISA as well as other laws relating to intelligence activities carried out by the Executive branch. Specifically, these measures are intended to codify existing privacy protections for the bulk telephone metadata program that are currently established through Court-approved minimization procedures or Executive branch policy. The measures in this bill also seek to enhance those privacy protections, where appropriate, by placing additional limits on the telephone metadata program that do not reduce its operational effectiveness. This legislation increases transparency—to the public and to the Congress—concerning the bulk telephone metadata

program, as well as other aspects of FISA, where it is possible to do so without compromising the efficacy of intelligence activities undertaken pursuant to FISA. Finally, the legislation also includes a series of measures—to include making the appointment of the Director of the NSA and the NSA Inspector General subject to Senate confirmation and requiring periodic review of Attorney General-approved procedures for intelligence collection under Executive order 12333—that do not specifically concern FISA or the bulk telephone metadata program, but which the Committee judges to be appropriate measures for improving both the implementation and oversight of intelligence activities.

Many of the measures contained in this legislation could not have been enacted absent the declassification of lawful intelligence activities that were, until recently, properly classified, as to do so would have revealed the programs to our adversaries and thereby compromised their effectiveness. These measures are possible now only because the impacted intelligence programs were publicly acknowledged following a series of unauthorized disclosures; however, this bill should not be construed as an endorsement of these unauthorized disclosures. The Committee is dismayed by leaks that have appeared in the media over the past several months concerning the bulk telephone metadata program, as well as other classified intelligence activities. The public disclosure of these programs is not a principled act of civil disobedience and has done grievous harm to the effectiveness of the programs involved and, hence, the nation's security.

All intelligence professionals take an oath to protect this country and sign non-disclosure agreements, which demand, at times, that those trusted with classified information keep it secret because to reveal it, whatever the motivation, is to provide details of classified intelligence sources and methods to our nation's enemies. This is true even when one disagrees with the sources and methods involved or the appropriateness of their classification. In fact, lawful means exist for true government "whistleblowers" to bring information regarding violations of law, or other concerns, to one of several Inspectors General throughout the government, or to Congress. These channels exist because, in a representative democracy, it is not for any one person to decide on his own which intelligence methods are wise or effective.

Recent media leaks concerning activities of the NSA have not exposed government wrongdoing. Rather, they have revealed to our adversaries lawful intelligence collection programs directed against valid foreign intelligence targets. Up until these programs were leaked, their implementation by NSA was an example of how our democratic system of checks and balances is intended to, and does, work. For example, the NSA telephone metadata program was approved by federal judges and overseen by Congress, where every member of the Senate had access to information concerning how the programs were conducted and an opportunity to voice objections and debate their efficacy. Some members did voice objections, but a substantially greater number weighed the relative privacy and security interests and chose to support these programs.

The unauthorized disclosures concerning these lawful programs have provided al-Qa'ida and others with a roadmap of how to better evade U.S. intelligence collection. Some would like to believe these disclosures have started a debate about the propriety and efficacy of NSA

surveillance programs but, in fact, to a substantial degree, recent unauthorized disclosures have ended the debate because, once disclosed, the programs at issue become substantially less effective. The nation will suffer as a result.

SECTION-BY-SECTION ANALYSIS AND EXPLANATION

The following is a section-by-section analysis and explanation of the FISA Improvements Act of 2013 that is being reported by the Committee.

Section 1. Short title

Section 1 states that the Act may be cited as the "*FISA Improvements Act of 2013*."

Section 2. Supplemental procedures for acquisition of certain business records for counterterrorism purposes

Section 2 clarifies the authority for bulk collection of records containing non-content metadata concerning the wire or electronic communications of United States persons. Section 2 adds two new provisions to Section 215 of the USA PATRIOT Act (Section 501 of FISA). The first provision (Section 501(i) of FISA) establishes a general prohibition on the use of Section 501 to acquire bulk wire or electronic communications records that concern the communications of U.S. persons if the order authorizing such collection does not name or otherwise identify individuals or facilities.

The second provision (Section 501(j) of FISA) provides authority for bulk collection otherwise prohibited by Section 501(i), provided the applicable Court order imposes certain supplemental procedures. Under this section, the acquisition of such records in bulk remains authorized under Section 215 of the USA PATRIOT Act but is subject to supplemental procedures that codify existing privacy protections for U.S. persons and adds new protections. Specifically, an order directed to the government authorizing the acquisition in bulk of wire or electronic communication records concerning the communications of United States persons from electronic communications service providers: (1) shall not authorize the acquisition of the content of any communication; (2) shall be effective for a period not to exceed 90 days; (3) shall mandate government retention of such records in accordance with Court-approved security procedures; (4) shall restrict analysts from accessing the data except to perform a query using a selector for which a recorded determination has been made that there is a reasonable articulable suspicion that the selector is associated with international terrorism or activities in preparation therefor; (5) shall require a record of each such determination and query; (6) shall limit the number of government personnel who can make such a determination or perform such a query; (7) shall record automatically, and subsequently report, the number of queries to Congress; (8) shall require the FISC to limit the number of tiers of contacts (i.e., "hops") that an analyst can receive in response to a query; (9) shall require that the FISC receives a written record of each determination, and allow for the Court to disapprove the determination, in which case the Court may order remedial action; and (10) shall limit retention of bulk metadata to five years, with a

further requirement of Attorney General-approval for queries of data that is more than three years old.

The Committee believes that, to the greatest extent practicable, all queries conducted pursuant to the authorities established under this section should be performed by Federal employees. Nonetheless, the Committee acknowledges that it may be necessary in some cases to use contractors to perform such queries. By using the term "government personnel" the Committee does not intend to prohibit such contractor use.

Section 2 also requires additional reporting to both Congress and the public concerning the Executive branch's use of Section 215, to include reporting concerning the number of targets and queries, as well as the number of investigative leads and probable cause orders initiated as a result of the telephone metadata program.

Section 3. Enhanced criminal penalties for unauthorized access to collected data

Section 3 establishes criminal penalties in Title 18 of the U.S. Code for unauthorized access to data repositories containing information acquired by the United States pursuant to an order of the FISC.

Section 4. Appointment of amicus curiae

Section 4 authorizes the FISC and the Foreign Intelligence Surveillance Court of Review (FISCR) to appoint *amicus curiae* to assist the Court in the consideration of applications that, in the opinion of the Court, present a novel or significant interpretation of the law.

Section 4 also requires the FISC and FISCR to designate one or more individuals, possessing the necessary clearances, who may be appointed to serve as *amicus curiae*.

Senators King, Collins, Warner, and Mikulski prepared this provision as an amendment and it was incorporated into the bill prior to markup.

Section 5. Consolidation of congressional oversight provisions under the Foreign Intelligence Surveillance Act of 1978

Section 5 consolidates five existing reporting requirements on FISA activities into a single semi-annual reporting requirement. In addition, this section adds measures intended to enhance overall transparency, to include measures intended to increase the availability of reports on FISA that are generated by the Executive branch to members of Congress not serving on the intelligence or judiciary committees, as well as measures intended to increase the availability of unclassified information contained in those reports to the public. Under this section, information previously required to be made public will continue to be made public.

Section 6. Restrictions on querying the contents of certain communications

Section 6 requires that the government document all queries of data acquired pursuant to Section 702 of FISA that use a U.S. Person's selector and provides that those queries may be conducted only if the purpose of the query is to obtain foreign intelligence information or information necessary to understand foreign intelligence information or to assess its importance. The section further requires that documentation of such queries will be available for review by the Department of Justice, appropriate Inspectors General, the FISC, and the Congress.

Section 6 does not limit the authority of law enforcement agencies to conduct queries of data acquired pursuant to Section 702 of FISA for law enforcement purposes.

This section recognizes the valid foreign intelligence need to conduct queries that use a U.S. Person selector, but seeks to ensure that appropriate limitations and oversight procedures are in place.

The Committee believes that, to the greatest extent practicable, all queries conducted pursuant to the authorities established under this section should be performed by Federal employees. Nonetheless, the Committee acknowledges that it may be necessary in some cases to use contractors to perform such queries. By using the term "government personnel" the Committee does not intend to prohibit such contractor use.

Section 7. Temporary targeting of persons other than United States persons traveling into the United States

Section 7 authorizes the government to continue collection for a 72-hour transitional period, where the collection is directed against a non-U.S. person target who travels into the United States while the target is the subject of collection that was lawfully initiated while the target was abroad. This provision is intended to provide the government with a grace period, to be used solely in exigent circumstances consistent with the reasonableness requirement of the Fourth Amendment, to enable the government to seek emergency authorization to maintain, rather than terminate, coverage of the target while such emergency authorization is sought. If a Court order is not issued, all collection after the time the target is known to have entered the U.S. must be deleted, unless the Attorney General determines that the information indicates a threat of death or serious bodily harm.

This provision responds to a gap in national security authorities. Under current law, collection directed against a lawful non-U.S. person target must terminate if that target is determined to have entered the United States, even if that target's presence in the country raises additional concerns. This mandatory cessation of surveillance exists whether coverage of the individual was authorized under Section 702 of FISA or under Executive order 12333, and creates a gap in coverage even where the government works expeditiously to develop the probable cause need to invoke the emergency procedures in FISA. Under this provision, collection directed against a non-U.S. person target may continue for a 72-hour period while the Executive branch seeks other surveillance authorities—to include emergency employment of

electronic surveillance under Section 105(e) of FISA. The Committee believes this situation is roughly analogous to the long-standing emergency procedures in FISA, through which the government, based on a finding of probable cause, can conduct electronic surveillance on an individual while it seeks Court approval.

Section 8. Confirmation of appointment of the Director of the National Security Agency

Section 8 amends the National Security Agency Act of 1959 to provide that the Director of the NSA shall be appointed by the President by and with the advice and consent of the Senate. Under present law and practice, the President appoints the Director of the NSA. The appointment has been indirectly subject to confirmation through Senate confirmation of the military officers who have been promoted into the position. Section 8 will make explicit that the filling of this key position in the Intelligence Community should be subject to Senate confirmation.

The Committee has had a long-standing interest in ensuring Senate confirmation of the Director of the NSA, and this requirement has previously been supported by the Senate. The Committee renews the requirement for Senate confirmation of the Director of the NSA in this Act in light of NSA's critical role in the national intelligence mission, particularly with respect to activities that may raise privacy concerns.

Through advice and consent, the Senate can enable the Congress to fulfill more completely its responsibility for providing oversight of the intelligence activities of the United States government and ensure that the NSA's responsibilities and foreign intelligence activities receive appropriate attention.

Section 8 does not alter the role of the Committee on Armed Services of the Senate in reviewing and approving the promotion or assignment of military officers. The Committee intends to approve a separate Senate Resolution that would dictate the roles of the Committee and the Armed Services Committee in considering the nomination of a new Director of the NSA, with the order of the committees' actions to be determined by whether the nominee is a military officer.

Finally, the section makes clear that the requirement for Senate confirmation applies prospectively. Therefore, the Director of the NSA on the date of enactment will not be affected by this section, which will apply initially to the appointment and confirmation of his successor.

Section 9. Presidential appointment and Senate confirmation of the Inspector General of the National Security Agency

Section 9 amends the Inspector General Act of 1978 (5 U.S.C. App.) to provide that the Inspector General of the NSA shall be appointed by the President by and with the advice and consent of the Senate. Under present law and practice, the Director of the NSA appoints the NSA Inspector General.

The Inspector General of the NSA performs a critical role in ensuring that the NSA carries out its national intelligence mission in full compliance with the law and applicable

policies and regulations. By requiring Presidential appointment and Senate confirmation of the NSA Inspector General, this provision will ensure the NSA Inspector General operates independently of the Director of the Agency in overseeing the activities of the NSA, particularly with respect to activities that may raise privacy concerns.

Senators Coats, Udall, Collins, Coburn, and Mikulski prepared this provision as an amendment, and it was incorporated into the bill prior to markup.

Section 10. Annual reports on violations of law or Executive order

Section 10 requires the DNI to report annually to the congressional intelligence committees on violations of law or Executive order by personnel of an element of the Intelligence Community that were identified during the previous calendar year. Under the National Security Act, the President is required to keep the congressional intelligence committees fully and currently informed of the intelligence activities of the United States government. Nonetheless, the Committee has determined that this annual reporting requirement is necessary to better ensure that the intelligence oversight committees of the House and Senate are made aware of violations of law or Executive order, including, in particular, violations of Executive order 12333 for activities not otherwise subject to FISA.

Section 11. Periodic review of Intelligence Community procedures for the acquisition, retention, and dissemination of intelligence

Section 11 mandates that the head of each element of the Intelligence Community conduct a review at least every five years of the Attorney General-approved procedures for intelligence collection that each Intelligence Community element is required to adopt pursuant to Section 2.3 of Executive order 12333. The procedures required by Executive order 12333 govern the handling of information concerning U.S. persons in all intelligence activities, including those also governed by FISA. It has come to the Committee's attention that some intelligence agencies have not substantively modified or updated their Attorney General-approved procedures in several decades. As a result, the procedures in place today pre-date advances in technology that have had a significant effect on the conduct of intelligence activities and on the privacy and civil liberties of U.S. persons. Further, it has come to the attention of the Committee that at least one Intelligence Community element does not have procedures in place. Section 11 reflects this Committee's belief that the adoption and periodic review of Attorney General-approved procedures for intelligence collection, which are required by Section 2.3 of Executive order 12333, is a priority that the Intelligence Community should work expeditiously to undertake.

Section 12. Privacy and Civil Liberties Oversight Board enhancements relating to the Foreign Intelligence Surveillance Act

Section 12 requires notification to the Privacy and Civil Liberties Oversight Board (PCLOB) of applications to the FISC that contain a new or significant interpretation of law and relate to efforts to protect the United States from terrorism. It also permits the PCLOB to

perform an assessment of those applications. In addition, Section 12 directs the PCLOB to conduct an annual review of the activities of the NSA related to information collection under FISA. Finally, Section 12 provides for communications services and office space to certain members of the PCLOB.

COMMITTEE ACTION

Votes on amendments to committee bill and this report

On October 29, 2013, a quorum being present, the Committee met to consider the bill and amendments. The Committee took the following actions:

By unanimous consent, the Committee made the Chairman and Vice Chairman's bill the base text for purposes of amendment. The Committee also authorized the staff to make technical and conforming changes in the bill and report following the completion of the mark-up.

By unanimous consent, the Committee agreed to amend the title of Section 3 of the bill to clarify more specifically what activity it will criminalize.

By a vote of 7 ayes to 8 noes the Committee rejected an amendment by Senator Rockefeller to establish a 3 year limit on the retention of bulk metadata. The votes on the amendment in person or by proxy were as follows: Chairman Feinstein—aye; Senator Rockefeller—aye; Senator Wyden—aye; Senator Mikulski—aye; Senator Udall—aye; Senator Warner—aye; Senator Heinrich—aye; Senator King—no; Vice Chairman Chambliss—no; Senator Burr—no; Senator Risch—no; Senator Coats—no; Senator Rubio—no; Senator Collins—no; Senator Coburn— no.

By a vote of 10 ayes to 5 noes the Committee agreed to an amendment by Senator Collins to enhance the role of the Privacy and Civil Liberties Oversight Board in overseeing certain intelligence activities authorized under FISA. The votes on the amendment in person or by proxy were as follows: Chairman Feinstein—aye; Senator Rockefeller—aye; Senator Wyden—aye; Senator Mikulski—aye; Senator Udall—aye; Senator Warner—aye; Senator Heinrich—aye; Senator King—aye; Vice Chairman Chambliss—no; Senator Burr—no; Senator Risch—no; Senator Coats—no; Senator Rubio—no; Senator Collins—aye; Senator Coburn—aye.

By a vote of 4 ayes to 11 noes the Committee rejected an amendment by Senator Wyden to express the intent of the Committee to hold additional open hearings on FISA during the 2013 calendar year. The votes on the amendment in person or by proxy were as follows: Chairman Feinstein—no; Senator Rockefeller—no; Senator Wyden—aye; Senator Mikulski—aye; Senator Udall—aye; Senator Warner—no; Senator Heinrich—aye; Senator King—no; Vice Chairman Chambliss—no; Senator Burr—no; Senator Risch—no; Senator Coats—no; Senator Rubio—no; Senator Collins—no; Senator Coburn—no.

By a vote of 6 ayes to 9 noes the Committee rejected an amendment by Senator Coburn to eliminate restrictions on the retention of bulk metadata. The votes on the amendment in

person or by proxy were as follows: Chairman Feinstein—no; Senator Rockefeller—no; Senator Wyden—no; Senator Mikulski—no; Senator Udall—no; Senator Warner—no; Senator Heinrich—no; Senator King—no; Vice Chairman Chambliss—no; Senator Burr—aye; Senator Risch—aye; Senator Coats—aye; Senator Rubio—aye; Senator Collins—aye; Senator Coburn—aye.

By a vote of 3 ayes to 12 noes the Committee rejected an amendment by Senator Udall to prohibit bulk collection of business records under Section 215 of the USA PATRIOT Act. The votes on the amendment in person or by proxy were as follows: Chairman Feinstein—no; Senator Rockefeller—no; Senator Wyden—aye; Senator Mikulski—no; Senator Udall—aye; Senator Warner—no; Senator Heinrich—aye; Senator King—no; Vice Chairman Chambliss—no; Senator Burr—no; Senator Risch—no; Senator Coats—no; Senator Rubio—no; Senator Collins—no; Senator Coburn—no.

By a vote of 15 ayes to 0 noes the Committee agreed to an amendment by Senator King to require the Director of National Intelligence to establish a technical procedure to record automatically the aggregate number of queries of bulk metadata and report that automatic recording to Congress on a quarterly basis. The votes on the amendment in person or by proxy were as follows: Chairman Feinstein—aye; Senator Rockefeller—aye; Senator Wyden—aye; Senator Mikulski—aye; Senator Udall—aye; Senator Warner—aye; Senator Heinrich—aye; Senator King—aye; Vice Chairman Chambliss—aye; Senator Burr—aye; Senator Risch—aye; Senator Coats—aye; Senator Rubio—aye; Senator Collins—aye; Senator Coburn—aye.

By a vote of 7 ayes to 8 noes the Committee rejected an amendment by Senator Wyden to require the public disclosure of any decision of the FISC that concerns a violation of the Constitution. The votes on the amendment in person or by proxy were as follows: Chairman Feinstein—no; Senator Rockefeller—no; Senator Wyden—aye; Senator Mikulski—aye; Senator Udall—aye; Senator Warner—aye; Senator Heinrich—aye; Senator King—aye; Vice Chairman Chambliss—no; Senator Burr—no; Senator Risch—no; Senator Coats—no; Senator Rubio—no; Senator Collins—aye; Senator Coburn—no.

By a vote of 3 ayes to 12 noes the Committee rejected an amendment by Senator Wyden to substitute the text of the bill with the text of S. 1551, the "Intelligence Oversight and Surveillance Reform Act." The votes on the amendment in person or by proxy were as follows: Chairman Feinstein—no; Senator Rockefeller—no; Senator Wyden—aye; Senator Mikulski—no; Senator Udall—aye; Senator Warner—no; Senator Heinrich—aye; Senator King—no; Vice Chairman Chambliss—no; Senator Burr—no; Senator Risch—no; Senator Coats—no; Senator Rubio—no; Senator Collins—no; Senator Coburn—no.

By a vote of 7 ayes to 8 noes the Committee rejected an amendment by Senator Heinrich to prohibit the collection of bulk cell site location information. The votes on the amendment in person or by proxy were as follows: Chairman Feinstein—no; Senator Rockefeller—aye; Senator Wyden—aye; Senator Mikulski—no; Senator Udall—aye; Senator Warner—aye; Senator Heinrich—aye; Senator King—aye; Vice Chairman Chambliss—no; Senator Burr—no; Senator Risch—no; Senator Coats—no; Senator Rubio—no; Senator Collins—aye; Senator Coburn—no.

Vote to report the committee bill

On October 31, 2013, a quorum being present, the Committee met to consider the bill, as amended. The Committee took the following actions:

The Committee voted to report the bill, as amended, by a vote of 11 ayes and 4 noes. The votes in person or by proxy were as follows: Chairman Feinstein—aye; Senator Rockefeller—aye; Senator Wyden—no; Senator Mikulski—aye; Senator Udall—no; Senator Warner—aye; Senator Heinrich—no; Senator King—aye; Vice Chairman Chambliss—aye; Senator Burr—aye; Senator Risch—aye; Senator Coats—aye; Senator Rubio—aye; Senator Collins—aye; Senator Coburn—no.

COMPLIANCE WITH RULE XLIV

Rule XLIV of the Standing Rules of the Senate requires publication of a list of any "congressionally directed spending item, limited tax benefit, and limited tariff benefit" that is included in the bill or the committee report accompanying the bill. Consistent with the determination of the Committee not to create any congressionally directed spending items or earmarks, none have been included in the bill, the report to accompany it, or the classified schedule of authorizations. The bill, report, and classified schedule also contain no limited tax benefits or limited tariff benefits.

ESTIMATE OF COSTS

Pursuant to paragraph 11(a)(3) of rule XXVI of the Standing Rules of the Senate, the Committee deems it impractical to include an estimate of the costs incurred in carrying out the provisions of this report due to the classified nature of the operations conducted pursuant to this legislation. On November 7, 2013, the Committee transmitted this bill to the Congressional Budget Office and requested it to conduct an estimate of the costs incurred in carrying out unclassified provisions.

EVALUATION OF REGULATORY IMPACT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee finds that no substantial regulatory impact will be incurred by implementing the provisions of this legislation.

CHANGES IN EXISTING LAWS

In the opinion of the Committee, it is necessary to dispense with the requirements of paragraph 12 of rule XXVI of the Standing Rules of the Senate in order to expedite the business of the Senate.

ADDITIONAL VIEWS OF SENATOR FEINSTEIN

The Intelligence Committee has conducted ongoing oversight of FISA since its enactment in 1978. Through that oversight, the Committee has been well aware of the implementation of FISA authorities, to include those under the Business Records provision (Section 215 of the USA PATRIOT Act and Section 501 of FISA) and the collection of electronic communications of non-U.S. Persons outside of the United States as authorized by Section 702 of FISA. That oversight has included among other things briefings and written information that we have received on the effectiveness of both programs, compliance issues that emerged in 2009 (regarding telephony metadata) and 2011 (regarding Section 702), and the efforts of the National Security Agency (NSA), the Department of Justice, and the Foreign Intelligence Surveillance Court to faithfully execute these programs under the Constitution and the law.

The Committee's review of these programs, as well as other aspects of FISA and signals intelligence collection conducted under Executive Order 12333, has been thorough and longstanding, but it has intensified since the disclosure of previously classified information through a series of press accounts beginning in June of this year. The Committee has held 10 hearings during this period,[1] plus numerous briefings and meetings with government officials, privacy advocates, and representatives of private sector companies.

The information we have received in the past several months has confirmed our previous understanding of these programs and has convinced the Committee that acquisition of telephone call records under the Business Records authority and the collection of foreign electronic communications under Section 702 of FISA should continue.

Prior to the unauthorized disclosures concerning the NSA's telephone metadata program, the Committee had reviewed options for shifting the operations of that program so as to keep the telephone records with telecommunications providers rather than acquire those records and store them at the NSA. The Committee reevaluated those options following public acknowledgement of the program by the Director of National Intelligence, but reached the same conclusion that such an alternative arrangement for the NSA program would not meet the Intelligence Community's operational needs.

Separately, the Committee, through its regular oversight, also has continued to receive briefings and intelligence products related to the threat to the United States from terrorism and the other national security challenges that require effective signals intelligence collection. It is clear that the threat has diversified, geographically around the world and in the number of groups involved. It is also clear that signals intelligence remains a critical part of our intelligence collection on these threats. The need for these intelligence programs, therefore, remains.

[1] Since the initial press reports based on materials leaked by Edward Snowden, the Committee has held hearings, briefings, and other full Committee meetings on NSA FISA operations and related intelligence activities on June 6, June 11, June 13, June 25, July 16, July 23, September 19, September 24, September 26 (in open session), and October 10.

Intelligence gathered pursuant to the programs under Section 215 of the USA PATRIOT Act and Section 702 of FISA, together with NSA's other authorities, has enabled the disruption of potential terrorist attacks at home and abroad. I strongly believe that the telephone call records program under the Section 215 Business Records provision reduces the chance of another 9/11-type attack on our homeland. In fact, the call records program has played a role in stopping roughly a dozen terror incidents in the United States. And it continues to contribute to our safety. To end the program at this time will substantially increase the risk of another catastrophic attack on the United States.

This is not a surveillance program. In the case of the call records program, neither individuals nor their phone conversations are being listened to. No one is being monitored. The call records collected do not include names, locations or other identifying characteristics of telephone calls. If the government wants to get the content of any conversations, it must obtain a warrant.

I recognize that for some people, any type of collection of their phone records creates unease, particularly those who are already distrustful of government. I also understand some believe Congress has not done enough to restrain or oversee these programs, though I strongly disagree with this view.

In approving the FISA Improvements Act of 2013, the Committee sought to codify existing privacy protections already mandated by the FISA Court and internal NSA regulations, and to impose new ones. We also sought to increase public understanding of the telephone metadata program, and to increase oversight conducted by Congress, the FISA Court, and the Privacy and Civil Liberties Oversight Board. These efforts are described throughout this report.

I recognize that the reforms in this legislation will be seen as insufficient by those who oppose the NSA's call records program. I do, however, wish to address two specific points of opposition with which I disagree.

- First, in reference to the call records program, some people will say that the FISA Improvements Act codifies an illegal program. It does not. This legislation does not provide any new legislative authority with which the government may acquire call records or any other information under Section 215—in fact, it narrows the existing authority for it. Section 2 of the FISA Improvements Act clearly prohibits the use of the Business Records authority to collect bulk communication records except through the supplemental procedures and restrictions required by this section, as are detailed in this report.

  As part of this previously classified program, in 2006, the Department of Justice sought approval from the FISA Court to collect call records in large number under the Section 215 Business Records provision. The FISA Court approved that request, and has reviewed and renewed that authority every 90 days for the past seven years. These renewal applications have been approved by at least 15 different federal court judges selected by the Chief Justice of the United States to serve on this Court.

The Department of Justice's legal analysis of the call records program has recently been publicly released, as have the two most recent opinions by the FISA Court as part of the reauthorization of the program every 90 days.

Critics of the program may dispute the legal reasoning, but there should be no disagreement that this program currently is authorized under law and has been determined to be legal and Constitutional by the Executive and Judicial branches.

- Second, there is a contention that this legislation authorizes the bulk collection of metadata from electronic communications in addition to telephone metadata. This is not the case.

  The Business Records provision under Section 501 of FISA has not been used for bulk electronic metadata collection (from emails, for example) in the past, and it is not the intent to authorize such collection here. The Department of Justice has previously sought and received authority to collect metadata from electronic communications under a separate provision—Section 402—of FISA (the pen register/trap and trace provision.) This Internet metadata collection program authorized by the FISA Court was discontinued in 2011 for operational and resource reasons and has not been restarted.

  To the extent such bulk electronic metadata collection is already permissible under Section 215, the effect of this legislation is to limit that collection, not to authorize it.

DIANNE FEINSTEIN

ADDITIONAL VIEWS OF SENATORS KING, COLLINS, WARNER AND MIKULSKI

Among other important provisions, this Bill contains two amendments we authored and/or supported, and which provide greater accountability, improved transparency and multiple layers of oversight to the FISA process.

The Amicus Curiae (friend of the court) provision ensures the Foreign Intelligence Surveillance Court has access to independent expertise to help the Court oversee sensitive intelligence programs while also safeguarding the Constitution's Fourth Amendment privacy protections. This provision enables the FISA Court to appoint an outside expert—including individuals with backgrounds in privacy, civil liberties, intelligence collection, telecommunications, or any other area in which the Court determines it could benefit from specialized legal or technical expertise—when a matter before the Court involves a novel or significant interpretation of the law that could have civil liberties implications.

The Privacy and Civil Liberties Oversight Board provision provides an additional layer of oversight to the FISA process by strengthening the oversight role of an independent, respected body focused on privacy and civil liberties—separate from other checks by all three branches of government including Congress and the Judiciary.

We need to be able to show the American people that the Intelligence Community can perform their primary function of protecting national security while also enhancing Americans' civil liberties and privacy protections guaranteed by the Constitution.

ANGUS KING
SUSAN M. COLLINS
MARK R. WARNER
BARBARA A. MIKULSKI

MINORITY VIEWS OF SENATORS WYDEN, UDALL AND HEINRICH

This bill represents the Senate Intelligence Committee's response to the recent disclosures of large-scale domestic surveillance programs, which were made earlier this year and which have triggered a national debate about surveillance policy. We are disappointed that this bill seems to work from the premise that the problem with these programs is not that they are overly intrusive, or that they were authorized under an anachronistic legal process, or that their usefulness has been greatly exaggerated, but rather that the law does not authorize and describe them as clearly as it should. To address this, this bill would codify the government's authority to collect the phone records of huge numbers of law-abiding Americans, and also to conduct warrantless searches for individual Americans' phone calls and emails. We respectfully but firmly disagree with this approach.

During the Intelligence Committee's consideration of this bill, we offered a number of amendments that would have made real reforms to US surveillance law and ensured the protection of both American security and American liberties. One of these amendments was a substitute amendment based on bipartisan surveillance reform legislation—the Intelligence Oversight and Surveillance Reform Act—that we have sponsored with a number of other Senators. This legislation would end the bulk collection of Americans' personal information while still allowing intelligence agencies to obtain information that they legitimately need for national security purposes.

Our legislation would also make a number of other needed reforms as well—in particular, it would prohibit the government from conducting warrantless "back-door searches" for Americans' communications under Section 702 of the Foreign Intelligence Surveillance Act, and it would create a Constitutional Advocate to present an opposing view when the Foreign Intelligence Surveillance Court is considering major questions of law or constitutional interpretation. In contrast, the bill that the Intelligence Committee is now reporting would give intelligence agencies wide latitude to conduct warrantless searches for Americans' phone calls and emails under Section 702. And while it would allow the Foreign Intelligence Surveillance Court to request amicus briefs from outside parties, this would unfortunately not guarantee that both sides of an argument would be presented to the Court on important cases.

Senator Udall also offered an amendment that would have specifically prohibited the dragnet collection of Americans' phone records and other personal information. In our judgment, collecting the phone records of huge numbers of law-abiding Americans is a major intrusion on these Americans' privacy. As Vice President Biden put it several years ago, "I don't have to listen to your phone calls to know what you're doing. If I know every single phone call you made, I'm able to determine every single person you talked to. I can get a pattern about your life that is very, very intrusive."

In our judgment, writing a law that permits the government to engage in this massive dragnet collection as long as there are rules about when officials can look at these phone records does not begin to solve the problem of overly intrusive domestic surveillance. When the Framers of the Constitution wrote the Bill of Rights, they did not say that government officials were

allowed to issue general warrants as long as they had rules about when they could look at the papers they seized. They believed that government officials should not seize the records of individual Americans without evidence of wrongdoing, and they embodied this principle in the Fourth Amendment.

In our view, the bulk collection of Americans' phone records is particularly egregious because we have yet to see evidence that it provides real value in protecting national security. Despite our repeated requests, the NSA still has not provided any examples of instances where they used this program to review phone records that could not have been obtained using a regular court order or emergency authorization and that provided useful information about terrorist activities. If government agencies identify a suspected terrorist, they should absolutely go to the relevant phone companies to get that person's phone records. But this can be done without collecting the records of huge numbers of ordinary Americans.

Senator Heinrich also offered an amendment that would have prohibited the NSA from collecting Americans' cell phone location information in bulk, while still permitting the government to acquire this information with an individualized warrant. We are particularly disappointed that this amendment was rejected by the Committee. NSA officials have testified that they are not engaged in the bulk collection of Americans' cell-site location information today, and have acknowledged collecting "samples" of this data in the past, but they have repeatedly declined to publicly answer questions from the three of us and other Senators about whether they have previously collected or made plans to collect this information in bulk, and they have specifically said that the NSA could collect this information in bulk in the future. By rejecting the Heinrich amendment and still approving the underlying bill, the Intelligence Committee has effectively voiced support for giving the executive branch the authority to turn the cell phone of every man, woman, and child in America into a tracking device. We strenuously disagree with this approach and we will continue to work to ensure that Americans' daily movements are not tracked without evidence of wrongdoing.

While we have served on the Intelligence Committee for varying lengths of time, all three of us can attest that our nation's intelligence professionals are overwhelmingly dedicated and patriotic men and women who make real sacrifices to help keep our country safe and free. We believe that they should be able to do their jobs secure in the knowledge that their agencies have the trust and confidence of the American people. This trust has been undermined by overly intrusive domestic surveillance programs and misleading statements made by senior officials over a period of many years. The way to rebuild this public trust is to reform surveillance law and end the dragnet surveillance of ordinary Americans in a way that preserves intelligence agencies' ability to collect information that is actually necessary for the preservation of American security, and we will continue to work with our Senate colleagues to achieve this goal.

RON WYDEN
MARK UDALL
MARTIN HEINRICH