110TH CONGRESS } HOUSE OF REPRESENTATIVES { REPT. 110–373
1st Session } { Part 2

RESPONSIBLE ELECTRONIC SURVEILLANCE THAT IS OVERSEEN, REVIEWED, AND EFFECTIVE ACT OF 2007 OR RESTORE ACT OF 2007

OCTOBER 12, 2007.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

---

Mr. REYES, from the Permanent Select Committee on Intelligence, submitted the following

R E P O R T

together with

MINORITY VIEWS

[To accompany H.R. 3773]

[Including cost estimate of the Congressional Budget Office]

The Permanent Select Committee on Intelligence, to whom was referred the bill (H.R. 3773) to amend the Foreign Intelligence Surveillance Act of 1978 to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Responsible Electronic Surveillance That is Overseen, Reviewed, and Effective Act of 2007" or "RESTORE Act of 2007".

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

SEC. 2. CLARIFICATION OF ELECTRONIC SURVEILLANCE OF NON-UNITED STATES PERSONS OUTSIDE THE UNITED STATES.

Section 105A of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended to read as follows:

"CLARIFICATION OF ELECTRONIC SURVEILLANCE OF NON-UNITED STATES PERSONS OUTSIDE THE UNITED STATES

"SEC. 105A. (a) FOREIGN TO FOREIGN COMMUNICATIONS.—Notwithstanding any other provision of this Act, a court order is not required for the acquisition of the contents of any communication between persons that are not United States persons and are not located within the United States for the purpose of collecting foreign intelligence information, without respect to whether the communication passes through the United States or the surveillance device is located within the United States.

"(b) COMMUNICATIONS OF NON-UNITED STATES PERSONS OUTSIDE OF THE UNITED STATES.—Notwithstanding any other provision of this Act other than subsection (a), electronic surveillance that is directed at the acquisition of the communications of a person that is reasonably believed to be located outside the United States and not a United States person for the purpose of collecting foreign intelligence information (as defined in paragraph (1) or (2)(A) of section 101(e)) by targeting that person shall be conducted pursuant to—

"(1) an order approved in accordance with section 105 or 105B; or

"(2) an emergency authorization in accordance with section 105 or 105C.".

SEC. 3. PROCEDURE FOR AUTHORIZING ACQUISITIONS OF COMMUNICATIONS OF NON-UNITED STATES PERSONS LOCATED OUTSIDE THE UNITED STATES.

Section 105B of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended to read as follows:

"PROCEDURE FOR AUTHORIZING ACQUISITIONS OF COMMUNICATIONS OF NON-UNITED STATES PERSONS LOCATED OUTSIDE THE UNITED STATES

"SEC. 105B. (a) IN GENERAL.—Notwithstanding any other provision of this Act, the Director of National Intelligence and the Attorney General may jointly apply to a judge of the court established under section 103(a) for an ex parte order, or the extension of an order, authorizing for a period of up to one year the acquisition of communications of persons that are reasonably believed to be located outside the United States and not United States persons for the purpose of collecting foreign intelligence information (as defined in paragraph (1) or (2)(A) of section 101(e)) by targeting those persons.

"(b) APPLICATION INCLUSIONS.—An application under subsection (a) shall include—

"(1) a certification by the Director of National Intelligence and the Attorney General that—

"(A) the targets of the acquisition of foreign intelligence information under this section are persons reasonably believed to be located outside the United States;

"(B) the targets of the acquisition are reasonably believed to be persons that are not United States persons;

"(C) the acquisition involves obtaining the foreign intelligence information from, or with the assistance of, a communications service provider or custodian, or an officer, employee, or agent of such service provider or custodian, who has authorized access to the communications to be acquired, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications; and

"(D) a significant purpose of the acquisition is to obtain foreign intelligence information (as defined in paragraph (1) or (2)(A) of section 101(e)); and

"(2) a description of—

"(A) the procedures that will be used by the Director of National Intelligence and the Attorney General during the duration of the order to deter-

mine that there is a reasonable belief that the targets of the acquisition are persons that are located outside the United States and not United States persons;

"(B) the nature of the information sought, including the identity of any foreign power against whom the acquisition will be directed;

"(C) minimization procedures that meet the definition of minimization procedures under section 101(h) to be used with respect to such acquisition; and

"(D) the guidelines that will be used to ensure that an application is filed under section 104, if otherwise required by this Act, when a significant purpose of an acquisition is to acquire the communications of a specific United States person reasonably believed to be located in the United States.

"(c) SPECIFIC PLACE NOT REQUIRED.—An application under subsection (a) is not required to identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed.

"(d) REVIEW OF APPLICATION.—Not later than 15 days after a judge receives an application under subsection (a), the judge shall review such application and shall approve the application if the judge finds that—

"(1) the proposed procedures referred to in subsection (b)(2)(A) are reasonably designed to determine whether the targets of the acquisition are located outside the United States and not United States persons;

"(2) the proposed minimization procedures referred to in subsection (b)(2)(C) meet the definition of minimization procedures under section 101(h); and

"(3) the guidelines referred to in subsection (b)(2)(D) are reasonably designed to ensure that an application is filed under section 104, if otherwise required by this Act, when a significant purpose of an acquisition is to acquire the communications of a specific United States person reasonably believed to be located in the United States.

"(e) ORDER.—

"(1) IN GENERAL.—A judge approving an application under subsection (d) shall issue an order—

"(A) authorizing the acquisition of the contents of the communications as requested, or as modified by the judge;

"(B) requiring the communications service provider or custodian, or officer, employee, or agent of such service provider or custodian, who has authorized access to the information, facilities, or technical assistance necessary to accomplish the acquisition to provide such information, facilities, or technical assistance necessary to accomplish the acquisition and to produce a minimum of interference with the services that provider, custodian, officer, employee, or agent is providing the target of the acquisition;

"(C) requiring such communications service provider, custodian, officer, employee, or agent, upon the request of the applicant, to maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished;

"(D) directing the Federal Government to—

"(i) compensate, at the prevailing rate, a person for providing information, facilities, or assistance pursuant to such order; and

"(ii) provide a copy of the portion of the order directing the person to comply with the order to such person; and

"(E) directing the applicant to follow—

"(i) the procedures referred to in subsection (b)(2)(A) as proposed or as modified by the judge;

"(ii) the minimization procedures referred to in subsection (b)(2)(C) as proposed or as modified by the judge; and

"(iii) the guidelines referred to in subsection (b)(2)(D) as proposed or as modified by the judge.

"(2) FAILURE TO COMPLY.—If a person fails to comply with an order issued under paragraph (1), the Attorney General may invoke the aid of the court established under section 103(a) to compel compliance with the order. Failure to obey an order of the court may be punished by the court as contempt of court. Any process under this section may be served in any judicial district in which the person may be found.

"(3) LIABILITY OF ORDER.—Notwithstanding any other law, no cause of action shall lie in any court against any person for providing any information, facilities, or assistance in accordance with an order issued under this subsection.

"(4) RETENTION OF ORDER.—The Director of National Intelligence and the court established under subsection 103(a) shall retain an order issued under

this section for a period of not less than 10 years from the date on which such order is issued.

"(5) ASSESSMENT OF COMPLIANCE WITH COURT ORDER.—At or before the end of the period of time for which an acquisition is approved by an order or an extension under this section, the court established under section 103(a) shall, not less frequently than once each quarter, assess compliance with the procedures and guidelines referred to in paragraph (1)(E) and review the circumstances under which information concerning United States persons was acquired, retained, or disseminated.".

SEC. 4. EMERGENCY AUTHORIZATION OF ACQUISITIONS OF COMMUNICATIONS OF NON-UNITED STATES PERSONS LOCATED OUTSIDE THE UNITED STATES.

Section 105C of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended to read as follows:

"EMERGENCY AUTHORIZATION OF ACQUISITIONS OF COMMUNICATIONS OF NON-UNITED STATES PERSONS LOCATED OUTSIDE THE UNITED STATES

"SEC. 105C. (a) APPLICATION AFTER EMERGENCY AUTHORIZATION.—As soon as is practicable, but not more than 7 days after the Director of National Intelligence and the Attorney General authorize an acquisition under this section, an application for an order authorizing the acquisition in accordance with section 105B shall be submitted to the judge referred to in subsection (b)(2) of this section for approval of the acquisition in accordance with section 105B.

"(b) EMERGENCY AUTHORIZATION.—Notwithstanding any other provision of this Act, the Director of National Intelligence and the Attorney General may jointly authorize the emergency acquisition of foreign intelligence information for a period of not more than 45 days if—

"(1) the Director of National Intelligence and the Attorney General jointly determine that—

"(A) an emergency situation exists with respect to an authorization for an acquisition under section 105B before an order approving the acquisition under such section can with due diligence be obtained;

"(B) the targets of the acquisition of foreign intelligence information under this section are persons reasonably believed to be located outside the United States;

"(C) the targets of the acquisition are reasonably believed to be persons that are not United States persons;

"(D) there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section will be acquired by targeting only persons that are reasonably believed to be located outside the United States and not United States persons;

"(E) the acquisition involves obtaining the foreign intelligence information from, or with the assistance of, a communications service provider or custodian, or an officer, employee, or agent of such service provider or custodian, who has authorized access to the communications to be acquired, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications;

"(F) a significant purpose of the acquisition is to obtain foreign intelligence information (as defined in paragraph (1) or (2)(A) of section 101(e));

"(G) minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h); and

"(H) there are guidelines that will be used to ensure that an application is filed under section 104, if otherwise required by this Act, when a significant purpose of an acquisition is to acquire the communications of a specific United States person reasonably believed to be located in the United States; and

"(2) the Director of National Intelligence and the Attorney General, or their designees, inform a judge having jurisdiction to approve an acquisition under section 105B at the time of the authorization under this section that the decision has been made to acquire foreign intelligence information.

"(c) INFORMATION, FACILITIES, AND TECHNICAL ASSISTANCE.—Pursuant to an authorization of an acquisition under this section, the Attorney General may direct a communications service provider, custodian, or an officer, employee, or agent of such service provider or custodian, who has the lawful authority to access the information, facilities, or technical assistance necessary to accomplish such acquisition to—

"(1) furnish the Attorney General forthwith with such information, facilities, or technical assistance in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that provider,

custodian, officer, employee, or agent is providing the target of the acquisition; and

"(2) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished.".

SEC. 5. OVERSIGHT OF ACQUISITIONS OF COMMUNICATIONS OF NON-UNITED STATES PERSONS LOCATED OUTSIDE OF THE UNITED STATES.

The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by inserting after section 105C the following new section:

"OVERSIGHT OF ACQUISITIONS OF COMMUNICATIONS OF NON-UNITED STATES PERSONS LOCATED OUTSIDE OF THE UNITED STATES

"SEC. 105D. (a) APPLICATION; PROCEDURES; ORDERS.—Not later than 7 days after an application is submitted under section 105B(a) or an order is issued under section 105B(e), the Director of National Intelligence and the Attorney General shall submit to the appropriate committees of Congress—

"(1) in the case of an application, a copy of the application, including the certification made under section 105B(b)(1); and

"(2) in the case of an order, a copy of the order, including the procedures and guidelines referred to in section 105B(e)(1)(E).

"(b) QUARTERLY AUDITS.—

"(1) AUDIT.—Not later than 120 days after the date of the enactment of this section, and every 120 days thereafter until the expiration of all orders issued under section 105B, the Inspector General of the Department of Justice shall complete an audit on the implementation of and compliance with the procedures and guidelines referred to in section 105B(e)(1)(E) and shall submit to the appropriate committees of Congress, the Attorney General, the Director of National Intelligence, and the court established under section 103(a) the results of such audit, including, for each order authorizing the acquisition of foreign intelligence under section 105B—

"(A) the number of targets of an acquisition under such order that were later determined to be located in the United States;

"(B) the number of persons located in the United States whose communications have been acquired under such order;

"(C) the number and nature of reports disseminated containing information on a United States person that was collected under such order; and

"(D) the number of applications submitted for approval of electronic surveillance under section 104 for targets whose communications were acquired under such order.

"(2) REPORT.—Not later than 30 days after the completion of an audit under paragraph (1), the Attorney General shall submit to the appropriate committees of Congress and the court established under section 103(a) a report containing the results of such audit.

"(c) COMPLIANCE REPORTS.—Not later than 60 days after the date of the enactment of this section, and every 120 days thereafter until the expiration of all orders issued under section 105B, the Director of National Intelligence and the Attorney General shall submit to the appropriate committees of Congress and the court established under section 103(a) a report concerning acquisitions under section 105B during the previous 120-day period. Each report submitted under this section shall include a description of any incidents of non-compliance with an order issued under section 105B(e), including incidents of non-compliance by—

"(1) an element of the intelligence community with minimization procedures referred to in section 105B(e)(1)(E)(i);

"(2) an element of the intelligence community with procedures referred to in section 105B(e)(1)(E)(ii);

"(3) an element of the intelligence community with guidelines referred to in section 105B(e)(1)(E)(iii); and

"(4) a person directed to provide information, facilities, or technical assistance under such order.

"(d) REPORT ON EMERGENCY AUTHORITY.—The Director of National Intelligence and the Attorney General shall annually submit to the appropriate committees of Congress a report containing the number of emergency authorizations of acquisitions under section 105C and a description of any incidents of non-compliance with an emergency authorization under such section.

"(e) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term 'appropriate committees of Congress' means—

"(1) the Permanent Select Committee on Intelligence of the House of Representatives;

"(2) the Select Committee on Intelligence of the Senate; and

"(3) the Committees on the Judiciary of the House of Representatives and the Senate.".

SEC. 6. FOREIGN INTELLIGENCE SURVEILLANCE COURT EN BANC.

Section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803) is amended by adding at the end the following new subsection:

"(g) In any case where the court established under subsection (a) or a judge of such court is required to review a matter under this Act, the court may, at the discretion of the court, sit en banc to review such matter and issue any orders related to such matter.".

SEC. 7. FOREIGN INTELLIGENCE SURVEILLANCE COURT MATTERS.

(a) AUTHORITY FOR ADDITIONAL JUDGES.—Section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a)) is amended—

(1) by inserting "(1)" after "(a)";

(2) in paragraph (1) (as so designated)—

(A) by striking "11" and inserting "15"; and

(B) by inserting "at least" before "seven of the United States judicial circuits"; and

(3) by designating the second sentence as paragraph (3) and indenting such paragraph, as so designated.

(b) CONSIDERATION OF EMERGENCY APPLICATIONS.—Such section is further amended by inserting after paragraph (1) (as designated by subsection (a)(1)) the following new paragraph:

"(2) A judge of the court shall make a determination to approve, deny, or modify an application submitted pursuant to section 105(f), section 304(e), or section 403 not later than 24 hours after the receipt of such application by the court.".

SEC. 8. REITERATION OF CHAPTERS 119 AND 121 OF TITLE 18, UNITED STATES CODE, AND FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 AS EXCLUSIVE MEANS BY WHICH DOMESTIC ELECTRONIC SURVEILLANCE MAY BE CONDUCTED.

(a) EXCLUSIVE MEANS.—Section 2511(2)(f) of title 18, United States Code, is amended by striking "and procedures in this chapter" and all that follows and inserting "and procedures in this chapter, chapters 121 and 206, and the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which electronic surveillance (as defined in section 101(f) of such Act), the interception of domestic wire, oral, and electronic communications, the accessing of stored electronic communications, and the installation and use of pen registers and trap and trace devices may be conducted.".

(b) AMENDMENT TO FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.—

(1) SECTION 109(a).—Section 109(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1809(a)) is amended by striking "authorized by statute" each place it appears and inserting "authorized by title I or IV of the Foreign Intelligence Surveillance Act (50 U.S.C. 1801–1811 and 1841–1846), or chapter 119, 121, or 206 of title 18, United States Code"

(2) SECTION 307(a).—Section 307(a)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1827(a)) is amended by striking "as authorized by statute" and inserting "as authorized by title III of the Foreign Intelligence Surveillance Act (50 U.S.C. 1821–1829) or Rule 41 of the Federal Rules of Criminal Procedure or any other warrant issued by a court of competent jurisdiction".

(c) AMENDMENT TO TITLE 18, UNITED STATES CODE.—Section 2511(2)(a)(ii)(B) of title 18, United States Code, is amended by striking "statutory requirements" and inserting "requirements under this chapter, chapters 121 and 206, and titles I and IV of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)".

SEC. 9. ENHANCEMENT OF ELECTRONIC SURVEILLANCE AUTHORITY IN WARTIME AND OTHER COLLECTION.

Sections 111, 309, and 404 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1811, 1829, and 1844) are amended by striking "Congress" and inserting "Congress or an authorization for the use of military force described in section 2(c)(2) of the War Powers Resolution (50 U.S.C. 1541(c)(2)) if such authorization contains a specific authorization for foreign intelligence collection under this section, or if the Congress is unable to convene because of an attack upon the United States".

SEC. 10. AUDIT OF WARRANTLESS SURVEILLANCE PROGRAMS.

(a) AUDIT.—Not later than 180 days after the date of the enactment of this Act, the Inspector General of the Department of Justice shall complete an audit of all programs of the Federal Government involving the acquisition of communications conducted without a court order on or after September 11, 2001, including the Terrorist Surveillance Program referred to by the President in a radio address on De-

cember 17, 2005. Such audit shall include acquiring all documents relevant to such programs, including memoranda concerning the legal authority of a program, authorizations of a program, certifications to telecommunications carriers, and court orders.

(b) REPORT.—

(1) IN GENERAL.—Not later than 30 days after the completion of the audit under subsection (a), the Inspector General shall 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 a report containing the results of such audit, including all documents acquired pursuant to conducting such audit.

(2) FORM.—The report under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(c) EXPEDITED SECURITY CLEARANCE.—The Director of National Intelligence shall ensure that the process for the investigation and adjudication of an application by the Inspector General or the appropriate staff of the Office of the Inspector General of the Department of Justice for a security clearance necessary for the conduct of the audit under subsection (a) is conducted as expeditiously as possible.

SEC. 11. RECORD-KEEPING SYSTEM ON ACQUISITION OF COMMUNICATIONS OF UNITED STATES PERSONS.

(a) RECORD-KEEPING SYSTEM.—The Director of National Intelligence and the Attorney General shall jointly develop and maintain a record-keeping system that will keep track of—

(1) the instances where the identity of a United States person whose communications were acquired was disclosed by an element of the intelligence community (as defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4))) that collected the communications to other departments or agencies of the United States; and

(2) the departments and agencies of the Federal Government and persons to whom such identity information was disclosed.

(b) REPORT.—The Director of National Intelligence and the Attorney General 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 a report on the record-keeping system created under subsection (a), including the number of instances referred to in paragraph (1).

SEC. 12. AUTHORIZATION FOR INCREASED RESOURCES RELATING TO FOREIGN INTELLIGENCE SURVEILLANCE.

There are authorized to be appropriated the Department of Justice, for the activities of the Office of the Inspector General, the Office of Intelligence Policy and Review, and other appropriate elements of the National Security Division, and the National Security Agency such sums as may be necessary to meet the personnel and information technology demands to ensure the timely and efficient processing of—

(1) applications and other submissions to the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a));

(2) the audit and reporting requirements under—

(A) section 105D of such Act; and

(B) section 10; and

(3) the record-keeping system and reporting requirements under section 11.

SEC. 13. ADDITIONAL PERSONNEL FOR PREPARATION AND CONSIDERATION OF APPLICATIONS FOR ORDERS APPROVING ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH.

(a) OFFICE OF INTELLIGENCE OF THE NATIONAL SECURITY DIVISION.—

(1) ADDITIONAL PERSONNEL.—The Office of Intelligence of the National Security Division of the Department of Justice is hereby authorized such additional personnel as may be necessary to carry out the prompt and timely preparation, modification, and review of applications under Foreign Intelligence Surveillance Act of 1978 for orders under that Act for foreign intelligence purposes.

(2) ASSIGNMENT.—The Attorney General shall assign personnel authorized by paragraph (1) to and among appropriate offices of the intelligence community (as defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4))) in order that such personnel may directly assist personnel of the Intelligence Community in preparing applications described in that paragraph and conduct prompt and effective oversight of the activities of such agencies under Foreign Intelligence Surveillance Court orders.

(b) DIRECTOR OF NATIONAL INTELLIGENCE.—

(1) ADDITIONAL LEGAL AND OTHER PERSONNEL.—The Director of National Intelligence is hereby authorized such additional legal and other personnel as may

be necessary to carry out the prompt and timely preparation of applications under the Foreign Intelligence Surveillance Act of 1978 for orders under that Act approving electronic surveillance for foreign intelligence purposes.

(2) ASSIGNMENT.—The Director of National Intelligence shall assign personnel authorized by paragraph (1) to and among the intelligence community (as defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4))), including the field offices of the Federal Bureau of Investigation, in order that such personnel may directly assist personnel of the intelligence community in preparing applications described in that paragraph.

(c) ADDITIONAL LEGAL AND OTHER PERSONNEL FOR FOREIGN INTELLIGENCE SURVEILLANCE COURT.—There is hereby authorized for the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a)) such additional staff personnel as may be necessary to facilitate the prompt and timely consideration by that court of applications under such Act for orders under such Act approving electronic surveillance for foreign intelligence purposes. Personnel authorized by this paragraph shall perform such duties relating to the consideration of such applications as that court shall direct.

(d) SUPPLEMENT NOT SUPPLANT.—The personnel authorized by this section are in addition to any other personnel authorized by law.

SEC. 14. DOCUMENT MANAGEMENT SYSTEM FOR APPLICATIONS FOR ORDERS APPROVING ELECTRONIC SURVEILLANCE.

(a) SYSTEM REQUIRED.—The Attorney General shall, in consultation with the Director of National Intelligence and the Foreign Intelligence Surveillance Court, develop and implement a secure, classified document management system that permits the prompt preparation, modification, and review by appropriate personnel of the Department of Justice, the Federal Bureau of Investigation, the National Security Agency, and other applicable elements of the United States Government of applications under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804) before their submission to the Foreign Intelligence Surveillance Court.

(b) SCOPE OF SYSTEM.—The document management system required by subsection (a) shall—

(1) permit and facilitate the prompt submittal of applications to the Foreign Intelligence Surveillance Court under the Foreign Intelligence Surveillance Act of 1978; and

(2) permit and facilitate the prompt transmittal of rulings of the Foreign Intelligence Surveillance Court to personnel submitting applications described in paragraph (1), and provide for the secure electronic storage and retrieval of all such applications and related matters with the court and for their secure transmission to the National Archives and Records Administration.

SEC. 15. TRAINING OF INTELLIGENCE COMMUNITY PERSONNEL IN FOREIGN INTELLIGENCE COLLECTION MATTERS.

The Director of National Intelligence shall, in consultation with the Attorney General—

(1) develop regulations to establish procedures for conducting and seeking approval of electronic surveillance, physical search, and the installation and use of pen registers and trap and trace devices on an emergency basis, and for preparing and properly submitting and receiving applications and orders under the Foreign Intelligence Surveillance Act of 1978; and

(2) prescribe related training on the Foreign Intelligence Surveillance Act of 1978 and related legal matters for the personnel of the applicable agencies of the intelligence community (as defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4))).

SEC. 16. INFORMATION FOR CONGRESS ON THE TERRORIST SURVEILLANCE PROGRAM AND SIMILAR PROGRAMS.

As soon as practicable after the date of the enactment of this Act, but not later than seven days after such date, the President shall fully inform each member of the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate on the following:

(1) The Terrorist Surveillance Program of the National Security Agency.

(2) Any program in existence from September 11, 2001, until the effective date of this Act that involves, whether in part or in whole, the electronic surveillance of United States persons in the United States for foreign intelligence or other purposes, and which is conducted by any department, agency, or other element of the United States Government, or by any entity at the direction of a department, agency, or other element of the United States Government, without fully complying with the procedures set forth in the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or chapter 119, 121, or 206 of title 18, United States Code.

SEC. 17. TECHNICAL AND CONFORMING AMENDMENTS.

(a) TABLE OF CONTENTS.—The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by striking the items relating to sections 105A, 105B, and 105C and inserting the following new items:

"Sec. 105A. Clarification of electronic surveillance of non-United States persons outside the United States.
"Sec. 105B. Procedure for authorizing acquisitions of communications of non-United States persons located outside the United States.
"Sec. 105C. Emergency authorization of acquisitions of communications of non-United States persons located outside the United States.
"Sec. 105D. Oversight of acquisitions of communications of non-United States persons located outside of the United States.".

(b) SECTION 103(e) OF FISA.—Section 103(e) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(e)) is amended—

(1) in paragraph (1), by striking "105B(h) or"; and

(2) in paragraph (2), by striking "105B(h) or".

(c) REPEAL OF CERTAIN PROVISIONS OF THE PROTECT AMERICA ACT OF 2007.—Sections 4 and 6 of the Protect America Act of 2007 (Public Law 110–55) are hereby repealed.

SEC. 18. SUNSET; TRANSITION PROCEDURES.

(a) SUNSET OF NEW PROVISIONS.—

(1) IN GENERAL.—Except as provided in paragraph (2), effective on December 31, 2009—

(A) sections 105A, 105B, 105C, and 105D of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) are hereby repealed; and

(B) the table of contents in the first section of such Act is amended by striking the items relating to sections 105A, 105B, 105C, and 105D.

(2) ACQUISITIONS AUTHORIZED PRIOR TO SUNSET.—Any authorization or order issued under section 105B of the Foreign Intelligence Surveillance Act of 1978, as amended by this Act, in effect on December 31, 2009, shall continue in effect until the date of the expiration of such authorization or order.

(b) ACQUISITIONS AUTHORIZED PRIOR TO ENACTMENT.—

(1) EFFECT.—Notwithstanding the amendments made by this Act, an authorization of the acquisition of foreign intelligence information under section 105B of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) made before the date of the enactment of this Act shall remain in effect until the date of the expiration of such authorization or the date that is 180 days after such date of enactment, whichever is earlier.

(2) REPORT.—Not later than 30 days after the date of the expiration of all authorizations of acquisition of foreign intelligence information under section 105B of the Foreign Intelligence Surveillance Act of 1978 (as added by Public Law 110–55) made before the date of the enactment of this Act in accordance with paragraph (1), the Director of National Intelligence and the Attorney General shall 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 a report on such authorizations, including—

(A) the number of targets of an acquisition under section 105B of such Act (as in effect on the day before the date of the enactment of this Act) that were later determined to be located in the United States;

(B) the number of persons located in the United States whose communications have been acquired under such section;

(C) the number of reports disseminated containing information on a United States person that was collected under such section;

(D) the number of applications submitted for approval of electronic surveillance under section 104 of such Act based upon information collected pursuant to an acquisition authorized under section 105B of such Act (as in effect on the day before the date of the enactment of this Act); and

(E) a description of any incidents of non-compliance with an authorization under such section, including incidents of non-compliance by—

(i) an element of the intelligence community with procedures referred to in subsection (a)(1) of such section;

(ii) an element of the intelligence community with minimization procedures referred to in subsection (a)(5) of such section; and

(iii) a person directed to provide information, facilities, or technical assistance under subsection (e) of such section.

(3) INTELLIGENCE COMMUNITY DEFINED.—In this subsection, the term "intelligence community" has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

PURPOSE

The purpose of the Responsible Electronic Surveillance That is Overseen, Reviewed, and Effective Act ("RESTORE Act") is to arm the intelligence community with powerful new authorities to conduct electronic surveillance of targets outside the United States, while restoring essential Constitutional protections for Americans that were sharply eroded when the President signed into law the so-called Protect America Act in August 2007.

COMMITTEE STATEMENT AND VIEWS

A. INTRODUCTION

More than six years after the horrific attacks on September 11, 2001, Osama bin Laden remains at large, and America continues to face an undiminished threat from al Qaeda and other radical Islamic terrorist organizations. The Committee believes that thwarting terrorist plots must remain the top priority for the U.S. intelligence community.

Electronic surveillance is an essential "early warning" tool for disrupting terrorist plots. The RESTORE Act provides the U.S. intelligence community with additional authorities to conduct electronic surveillance on U.S. soil when the targets of the surveillance are non-Americans overseas.

Authorizing this surveillance under a clear legal framework is essential, not only to ensure that law abiding Americans' private communications are protected, but also to provide clarity and legal protection to telecommunications companies that may be called upon to assist the government.

Two Constitutional provisions guide Congressional regulation of electronic surveillance on U.S. soil.

The first is Article I, Section 8, which states, "The Congress shall have Power To . . . provide for the common Defence." This broad authority vests in Congress the power, and the duty, to ensure that our armed forces, intelligence professionals, and law enforcement agencies have the resources and legal authorities to protect the nation.

The second guidepost is the Fourth Amendment, which states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The RESTORE Act represents a careful balance between the duty to provide for the common defense and the simultaneous duty to protect innocent Americans from unlawful seizures of their private communications by the government.

Some have suggested that protecting the Constitution would compromise the "flexibility" of the intelligence community to gain critical intelligence on our adversaries, that balancing security and liberty is a zero-sum game. The Committee firmly rejects that false choice. We do not believe that the only way to preserve American life is to sacrifice American liberty.

Indeed, the preservation of our Constitution has made America strong and secure for more than 200 years, and that no one should be permitted to frighten, or terrorize, America into weakening our Constitution. To do so would be to hand the terrorists a victory. Others may wish to surrender to terrorists in this fashion; this Committee never will.

B. BACKGROUND AND NEED FOR LEGISLATION

The Foreign Intelligence Surveillance Act (FISA) provides the legal framework for the government to collect specified types of foreign intelligence information.

1. FISA History

The Foreign Intelligence Surveillance Act of 1978 responded to revelations that U.S. intelligence agencies had conducted warrantless electronic surveillance of Americans in the name of national security. These abuses were initially illuminated in 1973 during the investigation of the Watergate break-in.[1] Two years later the Senate Select Committee to Study Governmental Operations with Respect to Intelligence, chaired by Senator Church (the "Church Committee"), concluded that every President since Franklin D. Roosevelt had conducted warrantless electronic surveillance, and that the National Security Agency had received from international cable companies "millions of cables which had been sent by American citizens in the reasonable expectation that they would be kept private."[2]

The Church Committee found that surveillance activities were conducted either in the absence of a statutory framework or under extremely broad interpretations of applicable law. It traced the "application of vague and elastic standards for wiretapping and bugging [that had] resulted in electronic surveillance which, by any objective measure, were improper and seriously infringed the Fourth Amendment Rights of both the targets and those with whom the targets communicated."[3] It reported that, although the executive orders that govern NSA's activities prohibit the agency from monitoring communications between persons within the United States, "NSA has interpreted 'foreign communications' to include communication where one terminal is outside the United States."[4]

The Church Committee report explained:

> Under this interpretation, NSA has, for many years, intercepted communications . . . even though the sender or receiver was an American. During the past decade, NSA increasingly broadened its interpretation of "foreign intelligence." . . . The overall consequence . . . was to break down the distinction between "foreign" and "domestic" intelligence. For example, in the 1960s, NSA began adding to its "watch lists," at the request of various intelligence agencies, the names of American suspected of involvement in civil disturbance or drug activity which had some foreign aspects. Second, Operation Shamrock, which began as

[1] Legislative History P.L. 95–511, p. 3908.
[2] Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities, Book II, April 26, 1976, p.12.
[3] Ibid, Book III, p. 32.
[4] Ibid, Book II, p. 104.

> an effort to acquire the telegrams of certain foreign targets, expanded so that NSA obtained from at least two cable companies essentially all cables to or from the United States, including millions of the private communications of Americans.[5]

In discussing the potential costs of abusive electronic surveillance, the report on P.L. 95–511 (FISA) noted in 1978:

> Also formidable—although incalculable—is the 'chilling effect' which warrantless electronic surveillance may have on the constitutional rights of those who were not targets of the surveillance, but who perceived themselves . . . as potential targets. . . . The exercise of political freedom depends in large measure on citizens' understanding that they will be able to be publicly active . . . without having to sacrifice the expectation of privacy that they rightfully hold.[6]

In 1978, Congress enacted FISA to strengthen both national security and the Constitutional rights of Americans. The two pillars of FISA are: (a) the requirement that a Foreign Intelligence Surveillance Court (FISC)—composed of independent federal judges—carefully oversee and authorize surveillance; and (b) the obligation that the Executive Branch must inform Congress on surveillance programs and activities.

FISA created procedural protections for United States persons while allowing less stringent standards for surveillance of foreign powers or agents of foreign powers. The drafters of the statute also imposed penalties on telecommunications companies that did not comply with the law's requirements. Since these companies are indispensable to the collection of foreign intelligence, imposing liability on them ensured that they would be meticulous in ensuring that the government was complying with the law in seeking surveillance assistance.

FISA's statutory scheme also provided for flexible procedures for emergencies and wartime.

For decades, FISA has served as an essential tool in our nation's intelligence collection efforts and was regarded as the exclusive means by which the government could conduct electronic surveillance for foreign intelligence purposes in the United States. As the Committee has learned in a variety of settings, information gained from FISA surveillance has kept the nation safe.

2. History of the "President's Program"

Soon after September 11, 2001, President Bush authorized the NSA to conduct a range of surveillance activities designed to protect the country from terrorism. Collectively, these activities were known inside the Administration as the "President's Program." On its face, the President's Program—which directed electronic surveillance at individuals abroad but also American citizens inside the United States—violated FISA's unambiguous provisions requiring a court order.

---

[5] Idem

[6] Legislative History, P.L. 95–511, p. 3909–3910.

Information about this Program was closely held within the Administration. For example, even though the NSA was directed to carry out this surveillance, Counsel to the Vice President David Addington—who helped draft the authorizations—did not permit Agency lawyers to read the Justice Department's opinions describing the legal justifications for violating FISA. In addition, Counsel for Intelligence Policy and Review, James Baker, testified before the Committee on September 20, 2007, that he was not even informed of the President's Program until after it was underway.

Certain members of Congress received periodic briefings on aspects of the President's Program, but the full Intelligence Committees in both chambers were not informed of these activities until the Spring of 2006. The Administration did not provide written authorizations and legal opinions to Members of Congress, and to this day those core documents have been withheld by the Administration.

The enormous secrecy surrounding the President's Program had little to do with the operational sensitivity of the collection methods. It was widely-known that the NSA was surveilling terrorists. What was "sensitive" was that the surveillance was not lawful: it violated a statute passed by Congress and signed into law by the President.

The Committee believes it is important to review, in depth, the full range of activities conducted under the President's Program. Committee Members and staff have received briefings from the Executive Branch on aspects of the Program. However, the Committee's oversight has been stymied by the refusal of the Administration to provide full documentation to the Committee.

The Committee does wish to clarify one misconception. Our concern is not with the men and women of NSA. The Committee believes that the NSA is a vital national security asset, staffed with some of our nation's best minds who serve patriotically pursuant to a strict ethic of legal compliance. Our concern is with those senior officials in the Administration who authorized the Program, shielded it from judicial and congressional oversight, and who—to this day—refuse to allow full transparency into its operations.

In hindsight, violating FISA was unnecessary. Had the Agencies come to Congress and requested modifications to FISA, Congress likely would have granted the authority.

The Committee notes that the Executive Branch came to Congress to request modifications to FISA numerous times. In the USA PATRIOT Act, Congress enhanced the ability of law enforcement officers to search electronic communications, including granting the authority to conduct roving wiretaps, extending the duration of FISA warrants, and expanding the scope of business records obtainable with a FISA Order. All told, the Patriot Act made some 20 changes to FISA, altering it fundamentally.

Congress repeatedly amended FISA to provide the Administration with the statutory authorization it needed uncover terrorist plots. Following the modifications provided in the initial PATRIOT Act, the Administration requested changes to FISA in the Intelligence Authorization Act of FY 2002, the Homeland Security Act of 2002, the Intelligence Reform and Terrorism Prevention Act in 2004, the USA PATRIOT Improvement and Reauthorizing Act of

2005, and the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006.

3. FISC Review

In December 2006, the Administration decided to place all aspects of the President's Program under review by the FISC.

On January 10, 2007, the FISC issued orders authorizing the government to target international communications of members of al Qaeda or associated terrorist organizations. Seven days later, on January 17, 2007, Attorney General Gonzales informed Congress, "As a result of these orders, any electronic surveillance that was occurring as part of the Terrorist Surveillance Program will now be conducted subject to the approval of the [FISC]."[7] Thus, the Administration decided not to reauthorize the President's Program, but to instead work under FISA.

As Director of National Intelligence ("DNI") Michael McConnell revealed to the El Paso Times,[8] when the time came to renew the program in May 2007, a second FISA judge issued a ruling that increased the burden on the NSA to provide information to the Court about individual foreign targets. The details of these orders remain classified.

4. An "Intelligence Gap"

In July 2007, the DNI informed the Committee that as a result of the FISC's May 2007 decision, the NSA was devoting precious resources providing information to the FISC about foreign targets. This, the DNI claimed, had caused a collection gap by reducing the number of foreign targets the NSA had the resources to surveil.

On July 18, 2007, the Chairman of the Committee wrote the President and urged him to devote all necessary resources to closing this critical intelligence gap. In addition, Committee Members and staff met with senior Intelligence Community officials to determine how to close this gap.

Throughout these discussions, the Committee was told of the excessive burden of devoting government resources to obtaining individual court orders for foreign targets when the collection occurs inside the United States with the assistance of U.S. communications companies.

The Administration strenuously urged that Congress remove any requirement to involve the FISC in electronic surveillance of foreign targets, even when they may be communicating with Americans.

The Committee rejected the Administration's request for three reasons. First, the collection occurred on U.S. soil, implicating the U.S. Constitution. Second, the purpose of the President's Program, as the President explained, was to collect communications where one end of the communication was in the United States, thus implicating the rights of Americans. Third, the collection involved well-known American communications companies, used by millions of Americans everyday. The Committee did not wish to authorize the government to access the companies' systems without any oversight.

---

[7] Letter from Attorney General Alberto Gonzales to Senate Judiciary Committee, January 17, 2007.

[8] El Paso Times, August 22, 2007.

Others urged the Committee to retain FISA's rule that the government be required to obtain an individual court order, based upon probable cause that the target of surveillance was a foreign power or agent of a foreign power, for any communication "to or from a person inside the United States"—even when the surveillance was directed at a person outside the United States.

The Committee also rejected this approach because non-United States Persons outside the United States do not require the Constitutional protection afforded to United States persons. Under well-established procedures, NSA is not required to obtain individual FISA orders against foreign targets when the collection occurs overseas. Therefore, the NSA should not be required to obtain individual FISA orders simply because the collection physically occurs inside the United States.

In the summer of 2007, the policy question before Committee was this: What rule should apply when the government seeks to acquire communications of persons overseas, when the collection occurs inside the United States and when the communication may involve a person inside the United States?

The Director of National Intelligence indicated that he had three priorities: (1) that individual "probable cause" determinations not be required for foreign targets; (2) that the Executive Branch be given authority to compel telecommunications companies to assist in surveillance of foreign targets; and (3) that individual "probable cause" orders continue to be required for U.S. Persons.

The Congressional leadership negotiated with Director McConnell and drafted legislation, H.R. 3356, that achieved these three objectives.

In the course of negotiations, Director McConnell made several other requests, including that authorization be expanded from terrorism-related intelligence to all foreign intelligence. In an effort to achieve a bipartisan agreement, the Congressional leadership agreed to this request as well.

However, instead of agreeing to a bipartisan solution that carefully balanced the national security and Constitutional considerations, the Director of National Intelligence shifted his stance. On August 3, 2007, he released a statement that he "must have certainty" to prevent "attacks that are being planned today to inflict mass casualties on the United States"—suggesting that the Democratic legislation would lead to such an outcome. (He later noted that he had not even read the legislation.)

H.R. 3356 received a majority of votes in the House, but it did not receive the required two-thirds vote to pass on the Suspension Calendar. On August 4, 2007, the House considered S. 1927, the Protect America Act ("PAA"), a bill drafted by the Administration. PAA passed the House and was signed into law.

The PAA authorized the Director of National Intelligence and the Attorney General to acquire foreign intelligence information "concerning" persons outside the United States for one year, as long as the acquisition was not electronic surveillance, involved the assistance of a telecommunications provider, and a significant purpose was to obtain foreign intelligence.

The impact of using the word "concerning" was that the Executive Branch could direct warrantless surveillance at Americans, as long as the information sought "concerned" a person abroad. FISA

experts testified before the Committee on September 18, 2007, that this breathtaking expansion of surveillance authority could be read to allow secret warrantless physical searches of Americans' homes, offices, computer records, and medical records. Administration officials have asserted that this was not their intent, while simultaneously insisting that the PAA's precise language must be reauthorized permanently.

The PAA eviscerates the FISC's oversight role. Under that statute, after 120 days, the FISC reviews the procedures and guidelines developed by the Attorney General under a "clearly erroneous" standard. This standard required the court to give the Administration's decision complete deference, effectively converting the Court into a "rubber stamp."

The PAA's prospective liability protection for telecommunications carriers was weaker than that in H.R. 3356 because it did not require a Court order, but only an Attorney General certification to compel cooperation.

The PAA authorities expire 180 days after enactment, requiring Congress to take further action if the authorities were to continue.

5. Post-PAA Enactment

Following enactment of the PAA, the Committee began meeting with representatives of the NSA, FBI, DOJ, and DNI to oversee the implementation of the new authorities. The leadership of the House committed to working on longer-term authorities for warrantless electronic surveillance that were more protective of the rights of Americans while providing the intelligence community with the tools it needed to protect the nation. The leadership also committed to bringing such a proposal to the floor quickly.

During Committee hearings, Members of the Committee sought to clarify the intent of ambiguous language in the PAA. The Committee also solicited the Administration's views on various legislative proposals.

Administration officials clarified that they did not seek authorization for: (1) warrantless searches of Americans' homes inside the United States; (2) warrantless searches by the FBI or NSA of domestic mail; (3) collection of medical or business records; (4) bulk collection of "call detail records"—also known as metadata—of every domestic phone call made by Americans. H.R. 3773, as reported by the Committee, does not authorize any of these activities.

More shocking, a senior Executive Branch official acknowledged to the Committee during an open hearing that the PAA authorizes warrantless spying on American soldiers abroad who may be communicating with their families back home. The following exchange took place between Ms. Wilson of New Mexico and Kenneth Wainstein, Assistant Attorney General for National Security Division of the Department of Justice:

> *Ms. Wilson*: "Thank you, Mr. Chairman. Mr. Wainstein, would the Protect America Act affect the e-mail of a soldier communicating with his family back home?"
> *Mr. Wainstein*: "Under certain circumstances, it would, yes. The Protect America Act allows us to target surveillance on persons overseas."

The RESTORE Act repeals the authority of the government under the PAA to conduct warrantless spying on American soldiers.

During testimony, Director McConnell indicated that he did not oppose raising the level of FISC review to a "reasonable" standard. He also did not oppose the Court reviewing minimization procedures. Further, he stated he did not oppose requiring an Inspector General to audit the program. These three features are incorporated into the RESTORE Act.

C. DISCUSSION OF LEGISLATION

The legislation supplements FISA by authorizing additional foreign intelligence collection against targets located overseas when the communication passes through the United States. It further empowers the FISC to approve certain aspects of the additional foreign intelligence collection to ensure that the privacy rights of Americans are protected.

1. Additional intelligence gathering authorities

The bill provides the Intelligence Community with the additional authority to engage in the collection of foreign intelligence information related to the national defense without obtaining individualized warrants for foreign targets, even when the collection occurs on a wire located in the United States.

First, it clarifies that FISA orders are not required to target communications between two foreign nationals overseas, even if the communication passes on a wire through the United States. This language ensures that the government may intercept the communications of terrorists and other threats to national security located overseas without seeking approval from the FISC if the communication does not involve a United States Person.

Second, the bill enhances FISA by allowing the Intelligence Community to target the communications of foreign nationals abroad without obtaining individualized warrants.

2. Protection of Constitutional rights for United States persons

The bill also mandates a meaningful and substantial role for the Court. The bill requires the FISC to review targeting procedures to ensure that they are reasonably designed to target only non-United States persons outside the United States. The FISC must also review minimization procedures that the Intelligence Community will use in policing its collection to ensure that the procedures meet the requirements under FISA. The FISC will also review the Intelligence Community's procedures to ensure that, when the government seeks to conduct electronic surveillance of a United States Person in the United States, it obtains a traditional individualized warrant from the FISA Court.

The bill requires that the FISC review and approve these procedures prior to collection. However, the bill includes a provision for emergency surveillance coverage under the new authority, which allows the Attorney General and the Director of National Intelligence, in emergencies, to begin surveillance and bring the procedures and guidelines to the FISA Court for review within 45 days.

The bill also makes clear that the new authorities cannot be used to target known United States Persons. In doing so, the bill provides protection to United States Persons abroad without confer-

ring any rights or privileges to persons within the United States who are neither United States Citizens nor lawfully admitted for permanent residence.

3. Liability protections for private sector

The bill provides additional liability protections for private sector actors that assist the government in facilitating surveillance authorized by court order pursuant to these new authorities.

4. Oversight and auditing of authorities

The bill includes substantial and meaningful congressional oversight and independent auditing of the activities undertaken by the Intelligence Community pursuant to the new authorities. It empowers the Department of Justice's Inspector General to ensure that Americans are not being targeted inappropriately by the Intelligence Community as a result of this additional authority, and it requires continuous and regular reporting to Congress and the FISC.

It also requires the Intelligence Community to provide Congress with information concerning past surveillance activities that were undertaken by the President outside of FISA.

5. Sunset

The bill sunsets on December 31, 2009, to allow Congress to review the Intelligence Community's use of the new authorities and the impact of those authorities on the Constitutional rights of Americans.

6. Streamlining provisions and additional resources

The bill modernizes and streamlines certain procedures for obtaining individualized FISA warrants for targets within the United States and authorizes additional resources for carrying out the new authorities and additional tasks related to oversight. It increases the size of the FISC to fifteen judges, and calls for more personnel and additional training for the Intelligence Community and others involved in implementing the new authorities under the bill.

7. Exclusivity of FISA

The bill reiterates that FISA is the exclusive means to conduct electronic surveillance for the purpose of foreign intelligence collection and provides stricter penalties for those who attempt to circumvent FISA.

8. Responding to the Minority's views

Instead of supporting a bill that will enhance our national security and restore Constitutional rights, the Minority has chosen to defend limitless spying on Americans, including our own soldiers. Defending the Administration's unchecked spying policies might play well with some, but we doubt history will judge it kindly.

The Minority lodges ten objections to H.R. 3773, each one more alarmist than the previous.

First, the Ranking Minority Member complains that the legislation fails to provide liability protection for telecommunications carriers allegedly involved in the President's Program. On May 31, 2007, the Chairman and the Ranking Minority Member signed a

letter to the Director of National Intelligence and the Attorney General requesting documents about the President's Program. These documents have not been provided. It is difficult for Congress to consider the issue of immunity until the Ranking Minority Member's own requests have been answered.

Second, they oppose the provision which states that foreign-to-foreign communications do not require a Court order. This is curious. We included this provision in H.R. 3773 because the Administration and Minority had claimed for months that this was the central defect with FISA.

Third, they are concerned that the scope of H.R. 3773 is too narrow. H.R. 3773 applies to intelligence collection "necessary to the national defense or the security of the United States." We understand that the PAA allows for unrestricted surveillance on academic institutions, think tanks, journalists, and U.S. service members abroad. We do not agree with this approach.

Fourth, they protest the creation of a record-keeping system at NSA designed to safeguard the communications of United States Persons. The fact that the Minority opposes accountability regarding the monitoring of Americans' communications raises the suspicion that the Minority is comfortable with the unrestricted dissemination of Americans' phone calls and emails throughout the federal government.

Fifth, the Minority complains about the lack of prospective liability protection for telecommunications companies in the RESTORE Act's emergency provision. We look forward to working with the Minority to address this issue.

Sixth, the Minority opposes a two-year sunset on H.R. 3773. However, we believe that because the RESTORE Act provides such powerful tools to the government, a sunset clause is an appropriate mechanism to require the Congress to revisit these tools in two years.

The seventh objection is the most troubling. They complain about "expand[ing] the role of the FISC into foreign intelligence collection overseas." The Court will not be involved in intelligence collection. The Court will be involved in approving the procedures drafted by the DNI to protect Americans. In fact, the FISC should be involved in oversight of foreign intelligence. That is why it is called a "Foreign Intelligence Surveillance Court."

They suggest that the legislation would require a "warrant" for listening to calls of terrorists abroad. This is flatly untrue. No individual warrant or court order is required for foreign targets under the RESTORE Act. The Court's role is to approve procedures to ensure that Americans are not targeted and that their Constitutional rights remain as they have for more than 200 years.

Eighth, the Minority opposes using the Department of Justice Inspector General for the purpose of auditing the surveillance. They decry imposing "non-Intelligence Community personnel into the work of the Intelligence Community." Under that rule, the House Permanent Select Committee on Intelligence would not be permitted to do its oversight work. Therein lies the difference; we support strong oversight.

Ninth, they oppose a requirement that the President provide information to Congress about the President's Program. The Committee's oversight of the program has been stymied by the White

House's refusal to provide the Ranking Minority Member with the relevant documentation that he and the Chairman requested on May 31. We cannot understand why the Minority opposes the Ranking Minority Member's request.

Tenth, they oppose the provision that reiterates FISA's exclusivity on the grounds that it could constitute an "unconstitutional infringement of the President's constitutional authority." The statutory language and legislative history of FISA makes clear that it was designed to limit the President's ability to conduct warrantless surveillance of Americans. FISA is not unconstitutional. The Minority's argument would apply with equal force to the Fourth Amendment itself—an argument too absurd to consider.

In addition to these complaints, the Committee has heard two additional complaints, which, although highly irregular, merit a reply.

Some have suggested that the bill as reported confers rights on terrorists who may have come into the United States under a visa and overstayed their visa. This is absolutely false. The RESTORE Act does nothing to alter the definition of U.S. Person in FISA, which includes U.S. citizens or persons lawfully admitted for permanent residence. The bill confers no right or privilege on temporary visa holders or illegal aliens.

Additionally, as part of a campaign to "put a human face" on the FISA discussion, some Republican officials have begun to suggest that FISA caused a delay in intercepting communications related to the missing soldiers from the 10th Mountain Division. This is as cynical as it is misleading. The RESTORE Act removes any requirement for individual warrants for foreign targets. But more fundamentally, as the DNI was forced to publicly acknowledge, the 9-hour delay in that case was caused by the Bush Administration's own bureaucracy. Although the Attorney General could have authorized surveillance in minutes, he was unreachable for nearly two hours because he was traveling in Texas. FISA does not preclude leadership and common sense in a time of crisis.

COMMITTEE HEARINGS AND BRIEFINGS

To date in the first session of the 110th Congress, the Committee has held seven hearings with respect to improvement of the FISA, two of which were held in open session and five of which were held in closed session.

The Committee held four hearings prior to passage of the PAA on August 4, 2007. On June 14, 2007, the Committee held a closed hearing to receive testimony from former Deputy Attorney General James B. Comey. On June 21, 2007, the Committee met in closed session to receive testimony from former Attorney General John Ashcroft. In a closed hearing on July 11, 2007, the Committee received testimony from General Michael Hayden, Director of the Central Intelligence Agency and former Director of the National Security Agency. On July 19, 2007, the Committee held a closed hearing to receive testimony from then-Attorney General Alberto Gonzales.

Three additional hearings were held after passage of the PAA. On September 6, 2007, the Committee met in closed session and received testimony from Mr. Robert S. Mueller, III, Director of the Federal Bureau of Investigation; Assistant Attorney General Ken-

neth Wainstein of the Department of Justice National Security Division; and Lieutenant General Keith Alexander, Director of the National Security Agency. On September 18, 2007, the Committee held an open hearing to receive testimony from Mr. James Baker, former Counsel for the Department of Justice Office of Intelligence Policy and Review and lecturer at Harvard Law School; Mr. Jim Dempsey, Policy Director for the Center for Democracy and Technology; Ms. Lisa Graves, Deputy Director of the Center for National Security Studies; and Mr. David Rivkin, a partner at Baker Hostetler. On September 20, 2007, the Committee again held an open hearing and received testimony from Vice Admiral J. Michael McConnell, U.S. Navy (Ret.), Director of National Intelligence; and Assistant Attorney General Wainstein from the Department of Justice National Security Division.

The Committee also received five briefings from the intelligence community on topics relating to FISA. On January 24, 2007, Assistant Attorney General Steven Bradbury, Assistant Attorney General Kenneth Wainstein, and National Security Agency General Counsel Vito Potenza briefed the Committee in a closed session. On July 24, 2007, the Committee was briefed by General Michael Hayden, Director of the Central Intelligence Agency and former Director of the National Security Agency. On July 31, 2007, the Committee, in a joint closed session with the House Committee on the Judiciary, was briefed by Vice Admiral J. Michael McConnell, U.S. Navy (Ret.), Director of National Intelligence. Director McConnell returned on August 2, 2007, to brief the entire House in a closed session, which was co-hosted by the Speaker of the House and the Committee. On September 11, 2007, Director McConnell again briefed the Committee in a closed session.

COMMITTEE CONSIDERATION AND ROLL CALL VOTES

On October 10, 2007, the Committee met in open and closed session and ordered the bill H.R. 3773 favorably reported, as amended.

OPEN SESSION

In open session, the Committee considered the text of the bill H.R. 3773.

The Committee considered the following amendments:

Mr. Boswell offered an amendment to provide retroactive immunity to communications service providers for any provision of information, assistance, or access to facilities in connection with an authorized communications intelligence program during the period beginning September 11, 2001, and ending on the date of the enactment of H.R. 3773. Mr. Boswell later withdrew his amendment.

Mr. Issa then introduced an amendment to provide retroactive immunity to communications service providers providing information, assistance, or access to facilities in connection with an authorized communications intelligence program during the period beginning September 11, 2001, and ending on the date of the enactment.

CLOSED SESSION

Mr. Hoekstra moved to close the meeting because national security would be endangered if the matters to be considered were dis-

closed. Mr. Gallegly seconded the motion, and the Chairman called for a record vote. The motion was agreed to by a record vote of 19 ayes to 1 no:

Voting aye: Mr. Reyes, Mr. Boswell, Mr. Cramer, Ms. Eshoo, Mr. Holt, Mr. Ruppersberger, Mr. Thompson, Ms. Schakowsky, Mr. Langevin, Mr. Murphy, Mr. Hoekstra, Mr. Everett, Mr. Gallegly, Ms. Wilson, Mr. Thornberry, Mr. McHugh, Mr. Tiahrt, Mr. Rogers, Mr. Issa.

Voting no: Mr. Hastings.

OPEN SESSION

After debate, the Committee returned to open session to complete consideration of the Issa Amendment.

It was not agreed to by a record vote of 9 ayes and 10 noes:

Voting aye: Mr. Boswell, Mr. Hoekstra, Mr. Everett, Mr. Gallegly, Mr. Thornberry, Mr. McHugh, Mr. Tiahrt, Mr. Rogers, Mr. Issa.

Voting no: Mr. Reyes, Mr. Hastings, Mr. Cramer, Ms. Eshoo, Mr. Holt, Mr. Ruppersberger, Mr. Thompson, Ms. Schakowsky, Mr. Langevin, Mr. Murphy.

Ms. Schakowsky offered an amendment to require that the Administration apply for an individual warrant when a "significant purpose" of the collection is to acquire the communications of a specific United States Person reasonably believed to be located in the United States.

Mr. Rogers then offered an amendment to modify the Schakowsky Amendment by striking the word "significant" and inserting the word "sole." The Rogers Secondary Amendment was not agreed to by a record vote of 8 ayes and 11 noes:

Voting aye: Mr. Hoekstra, Mr. Everett, Mr. Gallegly, Mr. Thornberry, Mr. McHugh, Mr. Tiahrt, Mr. Rogers, Mr. Issa.

Voting no: Mr. Reyes, Mr. Hastings, Mr. Boswell, Mr. Cramer, Ms. Eshoo, Mr. Holt, Mr. Ruppersberger, Mr. Thompson, Ms. Schakowsky, Mr. Langevin, Mr. Murphy.

Mr. Issa then offered an amendment to modify the Schakowsky Amendment by striking the word "significant" and inserting the word "primary." The Issa Secondary Amendment was not agreed to by a record vote of 8 ayes and 11 noes:

Voting aye: Mr. Hoekstra, Mr. Everett, Mr. Gallegly, Mr. Thornberry, Mr. McHugh, Mr. Tiahrt, Mr. Rogers, Mr. Issa.

Voting no: Mr. Reyes, Mr. Hastings, Mr. Boswell, Mr. Cramer, Ms. Eshoo, Mr. Holt, Mr. Ruppersberger, Mr. Thompson, Ms. Schakowsky, Mr. Langevin, Mr. Murphy.

The Committee then resumed debate on the Schakowsky Amendment. The Schakowsky Amendment was agreed to by a record vote of 11 ayes and 8 noes:

Voting aye: Mr. Reyes, Mr. Hastings, Mr. Boswell, Mr. Cramer, Ms. Eshoo, Mr. Holt, Mr. Ruppersberger, Mr. Thompson, Ms. Schakowsky, Mr. Langevin, Mr. Murphy.

Voting no: Mr. Hoekstra, Mr. Everett, Mr. Gallegly, Mr. Thornberry, Mr. McHugh, Mr. Tiahrt, Mr. Rogers, Mr. Issa.

The Committee then recessed for House floor votes and reconvened for business an hour later.

When the Committee reconvened, Mr. Holt offered three amendments en bloc under a unanimous consent agreement. The Holt

Amendment en bloc provides additional resources for the Foreign Intelligence Surveillance Court, establishes a document management system to streamline the system for handling FISA applications, requires FISA training for intelligence personnel, and clarifies FISA's wartime authority. The Holt Amendment en bloc also reiterates that FISA is the exclusive means of conducting electronic surveillance for foreign intelligence purposes and requires the Administration to fully inform Congress of the Terrorist Surveillance Program and any other surveillance program that does not comply with FISA.

The Committee adopted the Holt Amendment en bloc by a record vote of 12 ayes and 7 noes:

Voting aye: Mr. Reyes, Mr. Hastings, Mr. Boswell, Mr. Cramer, Ms. Eshoo, Mr. Holt, Mr. Ruppersberger, Mr. Tierney, Mr. Thompson, Ms. Schakowsky, Mr. Langevin, Mr. Murphy.

Voting no: Mr. Hoekstra, Mr. Everett, Mr. Gallegly, Ms. Wilson, Mr. Thornberry, Mr. Tiahrt, Mr. Issa.

Following consideration of the Holt Amendment, Mr. Langevin, along with Messrs. Tierney and Holt, offered an amendment to require that the Foreign Intelligence Surveillance Court conduct quarterly assessments of the targeting and minimization procedures and guidelines. The Langevin Amendment was agreed to on a record vote of 12 ayes and 7 noes:

Voting aye: Mr. Reyes, Mr. Hastings, Mr. Boswell, Mr. Cramer, Ms. Eshoo, Mr. Holt, Mr. Ruppersberger, Mr. Tierney, Mr. Thompson, Ms. Schakowsky, Mr. Langevin, Mr. Murphy.

Voting no: Mr. Hoekstra, Mr. Everett, Mr. Gallegly, Ms. Wilson, Mr. Thornberry, Mr. Tiahrt, Mr. Issa.

Mr. Holt offered an amendment to strike certain sections of the RESTORE Act. Following debate, Mr. Holt withdrew his amendment.

Mr. Hoekstra then offered an amendment in the nature of a substitute to repeal the sunset provisions of the Protect America Act and provide blanket retroactive immunity against prosecution of any corporation or person providing records or information to the Attorney General during the period beginning September 11, 2001, and ending with the date of enactment of the bill. The Hoekstra Amendment was not agreed to by a record vote of 7 ayes and 12 noes:

Voting aye: Mr. Hoekstra, Mr. Everett, Mr. Gallegly, Ms. Wilson, Mr. Thornberry, Mr. Tiahrt, Mr. Issa.

Voting no: Mr. Reyes, Mr. Hastings, Mr. Boswell, Mr. Cramer, Ms. Eshoo, Mr. Holt, Mr. Ruppersberger, Mr. Tierney, Mr. Thompson, Ms. Schakowsky, Mr. Langevin, Mr. Murphy.

The Committee then voted to report favorably the bill by a record vote of 12 ayes and 7 noes:

Voting aye: Mr. Reyes, Mr. Hastings, Mr. Boswell, Mr. Cramer, Ms. Eshoo, Mr. Holt, Mr. Ruppersberger, Mr. Tierney, Mr. Thompson, Ms. Schakowsky, Mr. Langevin, Mr. Murphy.

Voting no: Mr. Hoekstra, Mr. Everett, Mr. Gallegly, Ms. Wilson, Mr. Thornberry, Mr. Tiahrt, Mr. Issa.

SECTION-BY-SECTION ANALYSIS

Section 1. Short Title and Table of Contents

Section 2. Clarification of Electronic Surveillance of Non-United States Persons Outside the United States

105A(a) Clarifies that a court order is not required to collect the contents of communications between non-United States Persons located outside the United States (even when the surveillance device is located in the United States). Maintains the FISA section 101(f) definition of "electronic surveillance."

105A(b) Provides a procedure, subject to court review, for conducting electronic surveillance (as defined in section 101(f) of FISA) targeting persons reasonably believed to be outside the United States and not United States Persons when the purpose is to collect foreign intelligence information. (Note: this provision defines "foreign intelligence information" in accordance with the categories established in paragraphs (1) and (2)(A) of section 101(e) of FISA.)

Section 3. Procedure for Authorizing Acquisitions of Communications of Non-United States Persons Located Outside the United States

105B(a) Allows the Director of National Intelligence (DNI) and the Attorney General (AG) to jointly apply for a court order authorizing the collection of communications of persons reasonably believed to be outside the United States and not United States Persons.

105B(b) Requires that the contents of an application under 105B(a) include:

- A certification from the DNI and the AG that:

(A) The targets of the acquisition are reasonably believed to be outside the United States;

(B) The targets of the acquisition are reasonably believed to be persons who are not United States Persons;

(C) The acquisition involves obtaining the assistance of communications service providers; and

(D) A significant purpose of the acquisition is to obtain foreign intelligence information. (Note: this provision defines "foreign intelligence information" in accordance with the categories established in paragraphs (1) and (2)(A) of section 101(e) of FISA.)

- A description of:

(A) The procedures that will be used to determine that there is a reasonable belief that the targets of the acquisition are located outside the United States and are not United States Persons;

(B) The nature of the information sought (including the identity of any foreign power against whom the acquisition will be directed);

(C) Minimization procedures to be used that meet the requirements of section 101(h) of FISA; and

(D) The guidelines that will be used to ensure that the government obtains an individualized warrant when a significant purpose of the collection is to acquire the communications of a specific United States Person reasonably believed to be inside the United States.

105B(c) States that the application under 105B(a) is not required to identify the specific facilities, places, or premises where the acquisition will be directed.

105B(d) Requires a judge from the FISC to review an application under 105B(a) within 15 days of receiving such application and mandates approval of that application if the judge finds that:

- There are procedures reasonably designed to target only non-United States Persons located outside the United States;
- The proposed minimization procedures meet the definition of minimization procedures in section 101(h) of FISA; and
- There are guidelines reasonably designed to ensure that the government obtains an individualized warrant when a significant purpose of the collection is to acquire the communications of a specific United States Person reasonably believed to be inside the United States.

105B(e) Requires that a judge approving an application under 105B(d) issue an order:

- Authorizing the acquisition as requested or as modified by the judge;
- Compelling the assistance of a communications service provider who has authorized access to the information or facilities sought;
- Compelling such communications service provider to maintain security over any records concerning the acquisition;
- Directing the government to compensate the communications service provider and to provide a portion of the court order directing compliance to the communications service provider; and
- Directing the agency submitting the application to follow the procedures and guidelines outlined in 105B(b)(2).

This section also:

- Empowers the AG to invoke the aid of the FISC to compel the communications service provider to comply with the order;
- Establishes that no cause of action shall lie against any communications service provider for complying with an order issued under this section;
- Requires the DNI and the FISC to retain such orders for at least 10 years; and
- Requires the judge to assess compliance on a quarterly basis with the procedures and guidelines referred to in 105B(e)(1)(E).

Section 4. Emergency Authorization of Acquisitions of Communications of Non-United States Persons Located Outside the United States

105C(a) Requires that the DNI and the AG submit an application consistent with 105B within 7 days after authorizing emergency acquisition of foreign intelligence information.

105C(b) Allows the DNI and the AG to authorize emergency acquisition of foreign intelligence information for a period of no more than 45 days if:

- The DNI and the AG determine that an emergency situation exists;
- The targets of the acquisition are reasonably believed to be outside the United States;
- There are procedures in place reasonably designed to target only people outside the United States;

• The targets of the acquisition are not reasonably believed to be United States Persons;
• The acquisition involves obtaining the assistance of communications service providers;
• A significant purpose of the acquisition is to obtain foreign intelligence information (Note: this provision defines "foreign intelligence information" in accordance with the categories established in paragraphs (1) and (2)(A) of section 101(e) of FISA);
• Minimization procedures to be used meet the definition of minimization procedures under section 101(h) of FISA; and
• There are guidelines reasonably designed to ensure that the government obtains an individualized warrant when a significant purpose of the collection is to acquire the communications of a specific United States person reasonably believed to be located inside the United States.

This section also requires that the DNI and the AG inform a FISC judge of any emergency authorization to acquire foreign intelligence information under this section at the time such authorization is issued.

105C(c) Provides that the AG may direct a communications service provider to:
• Provide assistance in conducting the acquisition; and
• Maintain security over any records concerning the acquisition.

Section 5. Oversight of Acquisitions of Communications of Non-United States Persons Located Outside the United States

105D(a) Requires that the DNI and the AG submit each application submitted under 105B(a) (including the certification, procedures and guidelines) and any applicable order issued under 105B(e) to the appropriate committees of Congress within seven days after filing such application with the FISC.

105D(b) Requires the Inspector General of the Justice Department to conduct audits every 120 days into the implementation of and compliance with the guidelines referred to in 105B(e)(1)(E) and requires that the results of such audits be reported to the appropriate committees of Congress, and to the DNI, the AG, and the FISC.

This audit must include (for each order):
• The number of targets of acquisition determined to be located in the United States;
• The number of persons located in the United States whose communications have been acquired under such order;
• The number and nature of reports disseminated that contain information on a United States Person that was collected under such order; and
• The number of applications submitted for approval of electronic surveillance under section 104 of FISA whose communications were acquired under such order.

This section also requires that, no later than 30 days after the completion of such audit, the AG submit a report to the appropriate committees of Congress.

105D(c) Requires the DNI and the AG to submit to the appropriate committees of Congress and the FISC a compliance report that includes any incidents of non-compliance:

• By an element of the intelligence community with the procedures and guidelines referred to in 105B(e), or
• By a person directed to provide information, facilities, or technical assistance pursuant to an order issued under 105B.

This report must be submitted no later than 60 days after the enactment of the Act and every 120 days thereafter.

105D(d) Requires the DNI and the AG to annually a report to Congress reporting the number of emergency authorizations issued under 105C and a description of any incidents of non-compliance with an emergency authorization under 105C.

105D(e) Defines "appropriate committees of Congress" to mean the Intelligence and Judiciary Committees of the House and Senate:

Section 6. Foreign Intelligence Surveillance Court En Banc

Authorizes the FISC, at its discretion, to sit en banc.

Section 7. Foreign Intelligence Surveillance Court Matters

(a) Provides authority to increase the number of judges on the FISC from 11 to 15 and expand the number of judicial circuits from which those judges can be designated.

(b) Requires FISC judges to rule on emergency applications submitted under sections 105(f), 304(e) or 403 of FISA.

Section 8. Reiteration of Chapters 119 and 121 of Title 18, United States Code and FISA as Exclusive Means by which Domestic Electronic Surveillance May Be Conducted

(a) Expands the scope of FISA's exclusivity to include accessing of stored communications and the use of pen registers and trap and trace devices.

(b) Modifies FISA's penalty provisions to make explicit that any authorization for electronic surveillance must come from specific, enumerated statutes.

(c) Modifies the criminal statute governing electronic surveillance to require a written certification stating that specific, enumerated statutory requirements have been met in order to authorize a communications provider to provide assistance in conducting electronic surveillance.

Section 9. Enhancement of Electronic Surveillance Authority in Wartime and Other Collection

Amends the wartime provisions of FISA to authorize electronic surveillance without a warrant where (1) Congress issues a declaration of war, (2) Congress issues an authorization for the use of military force that explicitly authorizes electronic surveillance, or (3) Congress is unable to convene due to attack upon the United States.

Section 10. Audit of Warrantless Surveillance Programs

(a) Requires the Inspector General of the Justice Department, no later than 180 days after enactment of this Act, to conduct a comprehensive audit of all programs involving the acquisition of communications conducted without a court order since September 11, 2001, including the President's Program.

(b) Requires the Inspector General to submit to the appropriate committees of Congress a report containing the results of the audit, no later than 30 days after its completion—along with all documents acquired in conducting the audit. The report must be submitted in unclassified form but may include a classified annex.

(c) Requires the DNI to ensure that the process for granting necessary clearances for the Inspector General and appropriate staff is conducted as expeditiously as possible.

Section 11. Record-Keeping System on Interception of Communications Without Warrant of United States Persons

(a) Requires the DNI and the AG to jointly develop and maintain a system to record the instances where the identity of a United States Person was disclosed to other departments or agencies by an element of the intelligence community that collected the communications. The record-keeping system must also keep track of the persons to whom such identity was disclosed.

(b) Requires the DNI and the AG to report annually on the disclosures maintained in this record-keeping system.

Section 12. Authorization for Increased Resources Relating to Foreign Intelligence Surveillance

Authorizes appropriations for the Justice Department and the National Security Agency to meet resource demands associated with submitting applications to the FISC and fulfilling the audit, reporting, and record-keeping requirements in the Act.

Section 13. Additional Personnel for Preparation and Consideration of Applications for Orders Approving Electronic Surveillance and Physical Search

(a) Authorizes the Department of Justice to hire and assign additional personnel necessary for the prompt preparation, modification and review of FISA applications.

(b) Authorizes the Director of National Intelligence to hire and assign additional personnel necessary for the prompt preparation, modification and review of FISA applications.

(c) Authorizes the Foreign Intelligence Surveillance Court to hire additional personnel necessary for the prompt preparation, modification and review of FISA applications.

(d) Clarifies that the personnel authorized under this section are in addition to any other personnel authorized by law.

Section 14. Document Management System for Applications for Orders Approving Electronic Surveillance

(a) Requires the AG, in consultation with the DNI, to develop and implement a classified document management system for processing FISA applications.

(b) Requires that the system in subsection (a) facilitate prompt submission of FISA applications and rulings and provide for secure electronic storage and retrieval of all such applications.

Section 15. Training of Intelligence Community Personnel in Foreign Intelligence Collection Matters

Requires the DNI, in consultation with the AG, to establish procedures for conducting and seeking approval for (1) electronic sur-

veillance, (2) physical search, (3) pen registers, and (4) trap and trace devices on an emergency basis and to prescribe related training on FISA and other legal matters for applicable personnel.

Section 16. Information for Congress on the Terrorist Surveillance Program and Similar Programs

Requires the President to fully inform each member of the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence on the President's Program and any other electronic surveillance program of United States Persons in the United States in existence from September 11, 2001 until the effective date of this Act that did not comply with FISA.

Section 17. Technical and Conforming Amendments

(a) Amends the table of contents in FISA to remove section titles from the Protect America Act and to include new titles for sections 105A–D.

(b) Revises a reference in the FISA provisions relating to the FISC that had been added under the Protect America Act to provide the FISC jurisdiction to review applications submitted under 105B.

(c) Repeals the reporting requirements and transition procedures established under the Protect America Act.

Section 18. Sunset; Transition Procedures

(a)(1) Provides that, effective on December 31, 2009, sections 105A–D of FISA are repealed (along with their respective titles in the table of contents) and any amendments to section 103(e) and the table of contents of FISA prior to August 4, 2007 are repealed.

(a)(2) Provides that any authorization issued under 105B in effect on December 31, 2009 shall continue in effect until the date of expiration of that order.

(b)(1) Provides that any authorization issued under 105B that was in effect prior to the enactment of this act shall remain in effect until its expiration or until 180 days after the date of enactment (whichever is earlier).

(b)(2) Requires the DNI and the AG to issue a report on acquisitions conducted under the Protect America Act (to include the same information required in the audit of the RESTORE Act under 105D(b)(1)).

OVERSIGHT FINDINGS AND RECOMMENDATIONS

With respect to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee held two open hearings and five closed hearings, receiving testimony from outside experts, interested citizens, and Members of Congress. The Committee also received five briefings from senior officials of the Intelligence Community. The Committee reports that the findings and recommendations of the Committee are reflected in the bill, as reported by the Committee.

General Performance Goals and Objectives

In accordance with Clause (3)(c) of House rule XIII, the Committee's performance goals and objectives are reflected in the descriptive portions of this report.

Constitutional Authority Statement

The intelligence and intelligence-related activities of the United States government are carried out to support the national security interests of the United States.

Article 1, section 8 of the Constitution of the United States provides, in pertinent part, that 'Congress shall have power * * * to pay the debts and provide for the common defense and general welfare of the United States; * * *'; and 'to make all laws which shall be necessary and proper for carrying into execution * * * all other powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof.'

Unfunded Mandate Statement

Section 423 of the Congressional Budget and Impoundment Control Act (as amended by Section 101(a)(2) of the Unfunded Mandates Reform Act, P.L. 104–4) requires a statement of whether the provisions of the reported bill include unfunded mandates. In compliance with this requirement, the Committee has received a letter from the Congressional Budget Office included herein.

Applicability to the Legislative Branch

The Committee finds that the legislation does not address the terms of conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

Earmarks Statement

In accordance with clause 9 of rule XXI of the Rules of the House of Representatives, H.R. 3773 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of rule XXI.

Budget Authority and Congressional Budget Office Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, October 12, 2007.

Hon. Silvestre Reyes,
Chairman, Permanent Select Committee on Intelligence,
House of Representatives, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3773, the RESTORE Act of 2007.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Jason Wheelock.

Sincerely,

Peter R. Orszag.

Enclosure.

H.R. 3773, RESTORE Act of 2007

Summary: H.R. 3773 would modify a number of rules and procedures the government must follow when conducting electronic surveillance. In particular, the bill would amend several sections added to the Foreign Intelligence Surveillance Act (FISA) by the Protect America Act of 2007 (Public Law 110–55). Under H.R. 3773, the government would have to apply to the Foreign Intelligence Surveillance Court (FISC) for authorization to conduct electronic surveillance on non-U.S. persons (individuals who are neither U.S. citizens nor permanent residents) outside the United States in instances when such surveillance could result in the government also obtaining the communications of individuals in the United States.

Several sections of the bill would, if implemented, increase discretionary costs. However, CBO does not have access to the information necessary to estimate the impact on the budget of implementing H.R. 3773. Any changes in federal spending under the bill would be subject to the appropriation of the necessary funds. Enacting H.R. 3773 would not affect direct spending or revenues.

The Unfunded Mandates Reform Act (UMRA) excludes from the application of that act any legislative provisions that are necessary for national security. CBO has determined that section 4 of H.R. 3773, which would authorize certain electronic surveillance without a court order in an emergency situation, falls under that exclusion and has not reviewed it for intergovernmental or private-sector mandates.

Other provisions of H.R. 3773 contain intergovernmental mandates as defined in UMRA, but CBO estimates that any costs to state and local governments would fall well below the annual threshold established in that act ($66 million in 2007, adjusted annually for inflation).

H.R. 3773 contains a private-sector mandate as defined in UMRA because it would require certain entities to assist the government with electronic surveillance. Because CBO has no information about the prevalence of electronic surveillance and the cost of compliance for private-sector entities assisting the government with electronic surveillance, CBO has no basis for estimating the costs of the mandate or whether the costs would exceed the annual threshold established by UMRA for private-sector mandates ($131 million in 2007, adjusted annually for inflation).

Estimated cost to the Federal Government: The following provisions of H.R. 3773 could require additional appropriations:

- Section 10 would require the Inspector General of the Department of Justice (DOJ) to complete an audit of all programs involving the acquisition of communications conducted without a court order on or after September 11, 2001.
- Section 11 would require the Director of National Intelligence and the Attorney General to jointly develop and maintain a system to document instances when elements of the intelligence community have disclosed the identities of U.S. persons whose communications they have acquired to other departments or agencies of the U.S. government.

• Sections 12 and 14 would authorize additional personnel for DOJ, the Office of the Director of National Intelligence, the FISC, and the National Security Agency (NSA) to process and review applications for warrants under FISA. Section 12 would also authorize additional funding for information technology for DOJ and NSA to process applications for FISA warrants.

• Section 13 would require the Attorney General to develop a secure, classified document management system that would be used to prepare, modify, and review applications to the FISC.

CBO estimates that implementing those sections would increase the costs of conducting electronic surveillance, subject to the appropriation of the necessary funds. However, CBO does not have access to the information necessary to estimate the impact of those changes. Such an estimate would require information on the types and volume of surveillance that would be subject to those authorizations, and the current costs incurred by agencies involved in the FISA process.

Estimated impact on state, local, and tribal governments: The Unfunded Mandates Reform Act excludes from the application of that act any legislative provisions that are necessary for national security. CBO has determined that section 4 of H.R. 3773, which would authorize certain electronic surveillance without a court order in an emergency situation, falls under that exclusion and has not reviewed it for intergovernmental mandates.

Other provisions of H.R. 3773 contain intergovernmental mandates as defined in UMRA. The bill would protect individuals from lawsuits if they comply with certain federal requests for information. That exemption would preempt some state and local liability laws, but CBO estimates this preemption would impose no costs on state, local, or tribal governments.

The bill also would allow federal law enforcement officers to compel providers of communications services, including public institutions such as libraries, to provide information about their customers and users. Based on information from a recent survey of public libraries, CBO estimates that the number of requests likely would be small and that the total costs to public entities would be well below the annual threshold established in UMRA ($66 million in 2007, adjusted annually for inflation).

Estimated impact on the private sector: H.R. 3773 contains a private-sector mandate as defined in UMRA because it requires certain entities to assist the government with electronic surveillance. CBO has no basis for estimating the costs of the mandate or whether the costs would exceed the annual threshold established by UMRA for private-sector mandates ($131 million in 2007, adjusted annually for inflation).

H.R. 3773 would authorize the Director of National Intelligence and the Attorney General, after obtaining a judge's approval required under the bill, to require certain persons affiliated with a provider of communications services to provide the government with all information, facilities, and assistance necessary to conduct electronic surveillance and to acquire foreign intelligence. Because CBO has no information about how often such entities would be directed to provide assistance or the costs associated with providing assistance, CBO has no basis for estimating the costs of this mandate. The bill also would direct the government to compensate, at

the prevailing rate, a person for providing such information, facilities, or assistance.

Previous CBO estimate: On October 12, 2007, CBO also transmitted a cost estimate for H.R. 3773 as ordered reported by the House Committee on the Judiciary on October 10, 2007. The language of the two versions of the bill is similar, though this version of the bill contains some authorizations not included in the version approved by the Judiciary Committee.

This version of the bill would require the Attorney General to develop and maintain a secure, classified document management system for preparing and reviewing submissions to the FISC. In addition, this version of H.R. 3773 contains authorizations for additional personnel for the Office of the Director of National Intelligence and the Foreign Intelligence Surveillance Court that are not in the version approved by the Judiciary Committee. These additional authorizations could result in more costs than would result from the Judiciary Committee's version of H.R. 3773.

Estimate prepared by: Federal costs: Jason Wheelock; impact on state, local, and tribal governments: Neil Hood; impact on the private sector: Victoria Liu.

Estimate approved by: Peter H. Fontaine, Assistant Director for Budget Analysis.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

AN ACT To authorize electronic surveillance to obtain foreign intelligence information.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Foreign Intelligence Surveillance Act of 1978".

TABLE OF CONTENTS

TITLE I—ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

* * * * * * *

SEC. 103. (a)*(1)* The Chief Justice of the United States shall publicly designate [11] *15* district court judges from *at least* seven of the United States judicial circuits of whom no fewer than 3 shall reside within 20 miles of the District of Columbia who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this Act, except that no judge designated under this subsection shall hear the same application for electronic surveillance under this Act which has been denied previously by another judge designated under this subsection.

(2) A judge of the court shall make a determination to approve, deny, or modify an application submitted pursuant to section 105(f), section 304(e), or section 403 not later than 24 hours after the receipt of such application by the court.

(3) If any judge so designated denies an application for an order authorizing electronic surveillance under this Act, such judge shall provide immediately for the record a written statement of each reason for his decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established in subsection (b).

* * * * * * *

(e)(1) Three judges designated under subsection (a) who reside within 20 miles of the District of Columbia, or, if all of such judges are unavailable, other judges of the court established under subsection (a) as may be designated by the presiding judge of such court, shall comprise a petition review pool which shall have jurisdiction to review petitions filed pursuant to section [105B(h) or] 501(f)(1).

(2) Not later than 60 days after the date of the enactment of the USA PATRIOT Improvement and Reauthorization Act of 2005, the court established under subsection (a) shall adopt and, consistent with the protection of national security, publish procedures for the review of petitions filed pursuant to section [105B(h) or] 501(f)(1) by the panel established under paragraph (1). Such procedures shall provide that review of a petition shall be conducted in camera and shall also provide for the designation of an acting presiding judge.

* * * * * * *

(g) In any case where the court established under subsection (a) or a judge of such court is required to review a matter under this Act, the court may, at the discretion of the court, sit en banc to review such matter and issue any orders related to such matter.

* * * * * * *

[CLARIFICATION OF ELECTRONIC SURVEILLANCE OF PERSONS OUTSIDE THE UNITED STATES

[SEC. 105A. Nothing in the definition of electronic surveillance under section 101(f) shall be construed to encompass surveillance

directed at a person reasonably believed to be located outside of the United States.

[ADDITIONAL PROCEDURE FOR AUTHORIZING CERTAIN ACQUISITIONS CONCERNING PERSONS LOCATED OUTSIDE THE UNITED STATES

[SEC. 105B. (a) Notwithstanding any other law, the Director of National Intelligence and the Attorney General, may for periods of up to one year authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States if the Director of National Intelligence and the Attorney General determine, based on the information provided to them, that—

[(1) there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States, and such procedures will be subject to review of the Court pursuant to section 105C of this Act;

[(2) the acquisition does not constitute electronic surveillance;

[(3) the acquisition involves obtaining the foreign intelligence information from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications;

[(4) a significant purpose of the acquisition is to obtain foreign intelligence information; and

[(5) the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h).

[This determination shall be in the form of a written certification, under oath, supported as appropriate by affidavit of appropriate officials in the national security field occupying positions appointed by the President, by and with the consent of the Senate, or the Head of any Agency of the Intelligence Community, unless immediate action by the Government is required and time does not permit the preparation of a certification. In such a case, the determination of the Director of National Intelligence and the Attorney General shall be reduced to a certification as soon as possible but in no event more than 72 hours after the determination is made.

[(b) A certification under subsection (a) is not required to identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed.

[(c) The Attorney General shall transmit as soon as practicable under seal to the court established under section 103(a) a copy of a certification made under subsection (a). Such certification shall be maintained under security measures established by the Chief Justice of the United States and the Attorney General, in consultation with the Director of National Intelligence, and shall remain sealed unless the certification is necessary to determine the legality of the acquisition under section 105B.

[(d) An acquisition under this section may be conducted only in accordance with the certification of the Director of National Intel-

ligence and the Attorney General, or their oral instructions if time does not permit the preparation of a certification, and the minimization procedures adopted by the Attorney General. The Director of National Intelligence and the Attorney General shall assess compliance with such procedures and shall report such assessments to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate under section 108(a).

[(e) With respect to an authorization of an acquisition under section 105B, the Director of National Intelligence and Attorney General may direct a person to—

[(1) immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition in such a manner as will protect the secrecy of the acquisition and produce a minimum of interference with the services that such person is providing to the target; and

[(2) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such person wishes to maintain.

[(f) The Government shall compensate, at the prevailing rate, a person for providing information, facilities, or assistance pursuant to subsection (e).

[(g) In the case of a failure to comply with a directive issued pursuant to subsection (e), the Attorney General may invoke the aid of the court established under section 103(a) to compel compliance with the directive. The court shall issue an order requiring the person to comply with the directive if it finds that the directive was issued in accordance with subsection (e) and is otherwise lawful. Failure to obey an order of the court may be punished by the court as contempt of court. Any process under this section may be served in any judicial district in which the person may be found.

[(h)(1)(A) A person receiving a directive issued pursuant to subsection (e) may challenge the legality of that directive by filing a petition with the pool established under section 103(e)(1).

[(B) The presiding judge designated pursuant to section 103(b) shall assign a petition filed under subparagraph (A) to one of the judges serving in the pool established by section 103(e)(1). Not later than 48 hours after the assignment of such petition, the assigned judge shall conduct an initial review of the directive. If the assigned judge determines that the petition is frivolous, the assigned judge shall immediately deny the petition and affirm the directive or any part of the directive that is the subject of the petition. If the assigned judge determines the petition is not frivolous, the assigned judge shall, within 72 hours, consider the petition in accordance with the procedures established under section 103(e)(2) and provide a written statement for the record of the reasons for any determination under this subsection.

[(2) A judge considering a petition to modify or set aside a directive may grant such petition only if the judge finds that such directive does not meet the requirements of this section or is otherwise unlawful. If the judge does not modify or set aside the directive, the judge shall immediately affirm such directive, and order the recipient to comply with such directive.

[(3) Any directive not explicitly modified or set aside under this subsection shall remain in full effect.

[(i) The Government or a person receiving a directive reviewed pursuant to subsection (h) may file a petition with the Court of Review established under section 103(b) for review of the decision issued pursuant to subsection (h) not later than 7 days after the issuance of such decision. Such court of review shall have jurisdiction to consider such petitions and shall provide for the record a written statement of the reasons for its decision. On petition for a writ of certiorari by the Government or any person receiving such directive, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

[(j) Judicial proceedings under this section shall be concluded as expeditiously as possible. The record of proceedings, including petitions filed, orders granted, and statements of reasons for decision, shall be maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

[(k) All petitions under this section shall be filed under seal. In any proceedings under this section, the court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions of a submission, which may include classified information.

[(l) Notwithstanding any other law, no cause of action shall lie in any court against any person for providing any information, facilities, or assistance in accordance with a directive under this section.

[(m) A directive made or an order granted under this section shall be retained for a period of not less than 10 years from the date on which such directive or such order is made.

[SUBMISSION TO COURT REVIEW OF PROCEDURES

[SEC. 105C. (a) No later than 120 days after the effective date of this Act, the Attorney General shall submit to the Court established under section 103(a), the procedures by which the Government determines that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance. The procedures submitted pursuant to this section shall be updated and submitted to the Court on an annual basis.

[(b) No later than 180 days after the effective date of this Act, the court established under section 103(a) shall assess the Government's determination under section 105B(a)(1) that those procedures are reasonably designed to ensure that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance. The court's review shall be limited to whether the Government's determination is clearly erroneous.

[(c) If the court concludes that the determination is not clearly erroneous, it shall enter an order approving the continued use of such procedures. If the court concludes that the determination is clearly erroneous, it shall issue an order directing the Government to submit new procedures within 30 days or cease any acquisitions under section 105B that are implicated by the court's order.

[(d) The Government may appeal any order issued under subsection (c) to the court established under section 103(b). If such court determines that the order was properly entered, the court

shall immediately provide for the record a written statement of each reason for its decision, and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision. Any acquisitions affected by the order issued under subsection (c) of this section may continue during the pendency of any appeal, the period during which a petition for writ of certiorari may be pending, and any review by the Supreme Court of the United States.]

CLARIFICATION OF ELECTRONIC SURVEILLANCE OF NON-UNITED STATES PERSONS OUTSIDE THE UNITED STATES

SEC. 105A. (a) FOREIGN TO FOREIGN COMMUNICATIONS.—Notwithstanding any other provision of this Act, a court order is not required for the acquisition of the contents of any communication between persons that are not United States persons and are not located within the United States for the purpose of collecting foreign intelligence information, without respect to whether the communication passes through the United States or the surveillance device is located within the United States.

(b) COMMUNICATIONS OF NON-UNITED STATES PERSONS OUTSIDE OF THE UNITED STATES.—Notwithstanding any other provision of this Act other than subsection (a), electronic surveillance that is directed at the acquisition of the communications of a person that is reasonably believed to be located outside the United States and not a United States person for the purpose of collecting foreign intelligence information (as defined in paragraph (1) or (2)(A) of section 101(e)) by targeting that person shall be conducted pursuant to—

(1) an order approved in accordance with section 105 or 105B; or

(2) an emergency authorization in accordance with section 105 or 105C.

PROCEDURE FOR AUTHORIZING ACQUISITIONS OF COMMUNICATIONS OF NON-UNITED STATES PERSONS LOCATED OUTSIDE THE UNITED STATES

SEC. 105B. (a) IN GENERAL.—Notwithstanding any other provision of this Act, the Director of National Intelligence and the Attorney General may jointly apply to a judge of the court established under section 103(a) for an ex parte order, or the extension of an order, authorizing for a period of up to one year the acquisition of communications of persons that are reasonably believed to be located outside the United States and not United States persons for the purpose of collecting foreign intelligence information (as defined in paragraph (1) or (2)(A) of section 101(e)) by targeting those persons.

(b) APPLICATION INCLUSIONS.—An application under subsection (a) shall include—

(1) a certification by the Director of National Intelligence and the Attorney General that—

(A) the targets of the acquisition of foreign intelligence information under this section are persons reasonably believed to be located outside the United States;

(B) the targets of the acquisition are reasonably believed to be persons that are not United States persons;

(C) the acquisition involves obtaining the foreign intelligence information from, or with the assistance of, a communications service provider or custodian, or an officer, employee, or agent of such service provider or custodian, who has authorized access to the communications to be acquired, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications; and

(D) a significant purpose of the acquisition is to obtain foreign intelligence information (as defined in paragraph (1) or (2)(A) of section 101(e)); and

(2) a description of—

(A) the procedures that will be used by the Director of National Intelligence and the Attorney General during the duration of the order to determine that there is a reasonable belief that the targets of the acquisition are persons that are located outside the United States and not United States persons;

(B) the nature of the information sought, including the identity of any foreign power against whom the acquisition will be directed;

(C) minimization procedures that meet the definition of minimization procedures under section 101(h) to be used with respect to such acquisition; and

(D) the guidelines that will be used to ensure that an application is filed under section 104, if otherwise required by this Act, when a significant purpose of an acquisition is to acquire the communications of a specific United States person reasonably believed to be located in the United States.

(c) SPECIFIC PLACE NOT REQUIRED.—An application under subsection (a) is not required to identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed.

(d) REVIEW OF APPLICATION.—Not later than 15 days after a judge receives an application under subsection (a), the judge shall review such application and shall approve the application if the judge finds that—

(1) the proposed procedures referred to in subsection (b)(2)(A) are reasonably designed to determine whether the targets of the acquisition are located outside the United States and not United States persons;

(2) the proposed minimization procedures referred to in subsection (b)(2)(C) meet the definition of minimization procedures under section 101(h); and

(3) the guidelines referred to in subsection (b)(2)(D) are reasonably designed to ensure that an application is filed under section 104, if otherwise required by this Act, when a significant purpose of an acquisition is to acquire the communications of a specific United States person reasonably believed to be located in the United States.

(e) ORDER.—

(1) IN GENERAL.—A judge approving an application under subsection (d) shall issue an order—

(A) authorizing the acquisition of the contents of the communications as requested, or as modified by the judge;

(B) requiring the communications service provider or custodian, or officer, employee, or agent of such service provider or custodian, who has authorized access to the information, facilities, or technical assistance necessary to accomplish the acquisition to provide such information, facilities, or technical assistance necessary to accomplish the acquisition and to produce a minimum of interference with the services that provider, custodian, officer, employee, or agent is providing the target of the acquisition;

(C) requiring such communications service provider, custodian, officer, employee, or agent, upon the request of the applicant, to maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished;

(D) directing the Federal Government to—

(i) compensate, at the prevailing rate, a person for providing information, facilities, or assistance pursuant to such order; and

(ii) provide a copy of the portion of the order directing the person to comply with the order to such person; and

(E) directing the applicant to follow—

(i) the procedures referred to in subsection (b)(2)(A) as proposed or as modified by the judge;

(ii) the minimization procedures referred to in subsection (b)(2)(C) as proposed or as modified by the judge; and

(iii) the guidelines referred to in subsection (b)(2)(D) as proposed or as modified by the judge.

(2) FAILURE TO COMPLY.—If a person fails to comply with an order issued under paragraph (1), the Attorney General may invoke the aid of the court established under section 103(a) to compel compliance with the order. Failure to obey an order of the court may be punished by the court as contempt of court. Any process under this section may be served in any judicial district in which the person may be found.

(3) LIABILITY OF ORDER.—Notwithstanding any other law, no cause of action shall lie in any court against any person for providing any information, facilities, or assistance in accordance with an order issued under this subsection.

(4) RETENTION OF ORDER.—The Director of National Intelligence and the court established under subsection 103(a) shall retain an order issued under this section for a period of not less than 10 years from the date on which such order is issued.

(5) ASSESSMENT OF COMPLIANCE WITH COURT ORDER.—At or before the end of the period of time for which an acquisition is approved by an order or an extension under this section, the court established under section 103(a) shall, not less frequently than once each quarter, assess compliance with the procedures and guidelines referred to in paragraph (1)(E) and review the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

EMERGENCY AUTHORIZATION OF ACQUISITIONS OF COMMUNICATIONS OF NON-UNITED STATES PERSONS LOCATED OUTSIDE THE UNITED STATES

SEC. 105C. (a) APPLICATION AFTER EMERGENCY AUTHORIZATION.—As soon as is practicable, but not more than 7 days after the Director of National Intelligence and the Attorney General authorize an acquisition under this section, an application for an order authorizing the acquisition in accordance with section 105B shall be submitted to the judge referred to in subsection (b)(2) of this section for approval of the acquisition in accordance with section 105B.

(b) EMERGENCY AUTHORIZATION.—Notwithstanding any other provision of this Act, the Director of National Intelligence and the Attorney General may jointly authorize the emergency acquisition of foreign intelligence information for a period of not more than 45 days if—

(1) the Director of National Intelligence and the Attorney General jointly determine that—

(A) an emergency situation exists with respect to an authorization for an acquisition under section 105B before an order approving the acquisition under such section can with due diligence be obtained;

(B) the targets of the acquisition of foreign intelligence information under this section are persons reasonably believed to be located outside the United States;

(C) the targets of the acquisition are reasonably believed to be persons that are not United States persons;

(D) there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section will be acquired by targeting only persons that are reasonably believed to be located outside the United States and not United States persons;

(E) the acquisition involves obtaining the foreign intelligence information from, or with the assistance of, a communications service provider or custodian, or an officer, employee, or agent of such service provider or custodian, who has authorized access to the communications to be acquired, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications;

(F) a significant purpose of the acquisition is to obtain foreign intelligence information (as defined in paragraph (1) or (2)(A) of section 101(e));

(G) minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h); and

(H) there are guidelines that will be used to ensure that an application is filed under section 104, if otherwise required by this Act, when a significant purpose of an acquisition is to acquire the communications of a specific United States person reasonably believed to be located in the United States; and

(2) the Director of National Intelligence and the Attorney General, or their designees, inform a judge having jurisdiction to approve an acquisition under section 105B at the time of the

authorization under this section that the decision has been made to acquire foreign intelligence information.

(c) INFORMATION, FACILITIES, AND TECHNICAL ASSISTANCE.—Pursuant to an authorization of an acquisition under this section, the Attorney General may direct a communications service provider, custodian, or an officer, employee, or agent of such service provider or custodian, who has the lawful authority to access the information, facilities, or technical assistance necessary to accomplish such acquisition to—

(1) furnish the Attorney General forthwith with such information, facilities, or technical assistance in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that provider, custodian, officer, employee, or agent is providing the target of the acquisition; and

(2) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished.

OVERSIGHT OF ACQUISITIONS OF COMMUNICATIONS OF NON-UNITED STATES PERSONS LOCATED OUTSIDE OF THE UNITED STATES

SEC. 105D. (a) APPLICATION; PROCEDURES; ORDERS.—Not later than 7 days after an application is submitted under section 105B(a) or an order is issued under section 105B(e), the Director of National Intelligence and the Attorney General shall submit to the appropriate committees of Congress—

(1) in the case of an application, a copy of the application, including the certification made under section 105B(b)(1); and

(2) in the case of an order, a copy of the order, including the procedures and guidelines referred to in section 105B(e)(1)(E).

(b) QUARTERLY AUDITS.—

(1) AUDIT.—Not later than 120 days after the date of the enactment of this section, and every 120 days thereafter until the expiration of all orders issued under section 105B, the Inspector General of the Department of Justice shall complete an audit on the implementation of and compliance with the procedures and guidelines referred to in section 105B(e)(1)(E) and shall submit to the appropriate committees of Congress, the Attorney General, the Director of National Intelligence, and the court established under section 103(a) the results of such audit, including, for each order authorizing the acquisition of foreign intelligence under section 105B—

(A) the number of targets of an acquisition under such order that were later determined to be located in the United States;

(B) the number of persons located in the United States whose communications have been acquired under such order;

(C) the number and nature of reports disseminated containing information on a United States person that was collected under such order; and

(D) the number of applications submitted for approval of electronic surveillance under section 104 for targets whose communications were acquired under such order.

(2) REPORT.—Not later than 30 days after the completion of an audit under paragraph (1), the Attorney General shall submit to the appropriate committees of Congress and the court established under section 103(a) a report containing the results of such audit.

(c) COMPLIANCE REPORTS.—Not later than 60 days after the date of the enactment of this section, and every 120 days thereafter until the expiration of all orders issued under section 105B, the Director of National Intelligence and the Attorney General shall submit to the appropriate committees of Congress and the court established under section 103(a) a report concerning acquisitions under section 105B during the previous 120-day period. Each report submitted under this section shall include a description of any incidents of non-compliance with an order issued under section 105B(e), including incidents of non-compliance by—

(1) an element of the intelligence community with minimization procedures referred to in section 105B(e)(1)(E)(i);

(2) an element of the intelligence community with procedures referred to in section 105B(e)(1)(E)(ii);

(3) an element of the intelligence community with guidelines referred to in section 105B(e)(1)(E)(iii); and

(4) a person directed to provide information, facilities, or technical assistance under such order.

(d) REPORT ON EMERGENCY AUTHORITY.—The Director of National Intelligence and the Attorney General shall annually submit to the appropriate committees of Congress a report containing the number of emergency authorizations of acquisitions under section 105C and a description of any incidents of non-compliance with an emergency authorization under such section.

(e) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term "appropriate committees of Congress" means—

(1) the Permanent Select Committee on Intelligence of the House of Representatives;

(2) the Select Committee on Intelligence of the Senate; and

(3) the Committees on the Judiciary of the House of Representatives and the Senate.

[Effective on December 31, 2009, section 18(a)(1) of H.R. 3773 provides that sections 105A, 105B, 105C, and 105D of the Foreign Intelligence Surveillance Act of 1978 are repealed (including the items relating to such sections in the table of contents in the first section).]

* * * * * * *

PENALTIES

SEC. 109. (a) OFFENSE.—A person is guilty of an offense if he intentionally—

(1) engages in electronic surveillance under color of law except as [authorized by statute] *authorized by title I or IV of the Foreign Intelligence Surveillance Act (50 U.S.C. 1801–1811 and 1841–1846), or chapter 119, 121, or 206 of title 18, United States Code*; or

(2) disclose or uses information obtained under color of law by electronic surveillance, knowing or having reason to known that the information was obtained through electronic surveillance not [authorized by statute] *authorized by title I or IV of*

the Foreign Intelligence Surveillance Act (50 U.S.C. 1801–1811 and 1841–1846), or chapter 119, 121, or 206 of title 18, United States Code.

* * * * * * *

AUTHORIZATION DURING TIME OF WAR

SEC. 111. Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the [Congress] *Congress or an authorization for the use of military force described in section 2(c)(2) of the War Powers Resolution (50 U.S.C. 1541(c)(2)) if such authorization contains a specific authorization for foreign intelligence collection under this section, or if the Congress is unable to convene because of an attack upon the United States*.

* * * * * * *

TITLE III—PHYSICAL SEARCHES WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

* * * * * * *

PENALTIES

SEC. 307. (a) A person is guilty of an offense if he intentionally—

(1) under color of law for the purpose of obtaining foreign intelligence information, executes a physical search within the United States except [as authorized by statute] *as authorized by title III of the Foreign Intelligence Surveillance Act (50 U.S.C. 1821–1829) or Rule 41 of the Federal Rules of Criminal Procedure or any other warrant issued by a court of competent jurisdiction*; or

* * * * * * *

AUTHORIZATION DURING TIME OF WAR

SEC. 309. Notwithstanding any other provision of law, the President, through the Attorney General, may authorize physical searches without a court order under this title to acquire foreign intelligence information for a period not to exceed 15 calendar days following a declaration of war by the [Congress] *Congress or an authorization for the use of military force described in section 2(c)(2) of the War Powers Resolution (50 U.S.C. 1541(c)(2)) if such authorization contains a specific authorization for foreign intelligence collection under this section, or if the Congress is unable to convene because of an attack upon the United States*.

* * * * * * *

TITLE IV—PEN REGISTERS AND TRAP AND TRACE DEVICES FOR FOREIGN INTELLIGENCE PURPOSES

* * * * * * *

AUTHORIZATION DURING TIME OF WAR

SEC. 404. Notwithstanding any other provision of law, the President, through the Attorney General, may authorize the use of a pen register or trap and trace device without a court order under this title to acquire foreign intelligence information for a period not to exceed 15 calendar days following a declaration of war by [Congress] *Congress or an authorization for the use of military force described in section 2(c)(2) of the War Powers Resolution (50 U.S.C. 1541(c)(2)) if such authorization contains a specific authorization for foreign intelligence collection under this section, or if the Congress is unable to convene because of an attack upon the United States*.

* * * * * * *

SECTION 2511 OF TITLE 18, UNITED STATES CODE

§ 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) * * *

(2)(a)(i) * * *

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with—

(A) * * *

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all [statutory requirements] *requirements under this chapter, chapters 121 and 206, and titles I and IV of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)* have been met, and that the specified assistance is required,

* * * * * * *

(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, [and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.] *and procedures in this chapter, chapters 121 and 206 of this title, and the Foreign Intelligence Surveillance Act of 1978 (50*

U.S.C. 1801 et seq.) shall be the exclusive means by which electronic surveillance (as defined in section 101(f) of such Act), the interception of domestic wire, oral, and electronic communications, the accessing of stored electronic communications, and the installation and use of pen registers and trap and trace devices may be conducted.

* * * * * * *

PROTECT AMERICA ACT OF 2007

* * * * * * *

[SEC. 4. REPORTING TO CONGRESS.

[On a semi-annual basis the Attorney General shall inform the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives, concerning acquisitions under this section during the previous 6-month period. Each report made under this section shall include—

[(1) a description of any incidents of non-compliance with a directive issued by the Attorney General and the Director of National Intelligence under section 105B, to include—

[(A) incidents of non-compliance by an element of the Intelligence Community with guidelines or procedures established for determining that the acquisition of foreign intelligence authorized by the Attorney General and Director of National Intelligence concerns persons reasonably to be outside the United States; and

[(B) incidents of noncompliance by a specified person to whom the Attorney General and Director of National Intelligence issue a directive under this section; and

[(2) the number of certifications and directives issued during the reporting period.]

* * * * * * *

[SEC. 6. EFFECTIVE DATE; TRANSITION PROCEDURES.

[(a) EFFECTIVE DATE.—Except as otherwise provided, the amendments made by this Act shall take effect immediately after the date of the enactment of this Act.

[(b) TRANSITION PROCEDURES.—Notwithstanding any other provision of this Act, any order in effect on the date of enactment of this Act issued pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall remain in effect until the date of expiration of such order, and, at the request of the applicant, the court established under section 103(a) of such Act (50 U.S.C. 1803(a)) shall reauthorize such order as long as the facts and circumstances continue to justify issuance of such order under the provisions of the Foreign Intelligence Surveillance Act of 1978, as in effect on the day before the applicable effective date of this Act. The Government also may file new applications, and the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a)) shall enter orders granting such applications pursuant to such Act, as long as the application meets the requirements set forth under the provisions of such Act

as in effect on the day before the effective date of this Act. At the request of the applicant, the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a)), shall extinguish any extant authorization to conduct electronic surveillance or physical search entered pursuant to such Act. Any surveillance conducted pursuant to an order entered under this subsection shall be subject to the provisions of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as in effect on the day before the effective date of this Act.

[(c) SUNSET.—Except as provided in subsection (d), sections 2, 3, 4, and 5 of this Act, and the amendments made by this Act, shall cease to have effect 180 days after the date of the enactment of this Act.

[(d) AUTHORIZATIONS IN EFFECT.—Authorizations for the acquisition of foreign intelligence information pursuant to the amendments made by this Act, and directives issued pursuant to such authorizations, shall remain in effect until their expiration. Such acquisitions shall be governed by the applicable provisions of such amendments and shall not be deemed to constitute electronic surveillance as that term is defined in section 101(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(f)).]

MINORITY VIEWS

INTRODUCTION

We cannot join with our majority colleagues in supporting H.R. 3773, the "RESTORE Act." This bill is clearly designed to meet a political need of the Democrat majority, and not the country's needs during a time of continued struggle against radical jihadists and other hostile acts by foreign powers. This bill fails to provide the effective tools that the Intelligence Community has repeatedly stated it needs to efficiently collect foreign intelligence information to prevent and disrupt terrorist plots.

In H.R. 3773, Congress would expressly legislate, for the first time, that a United States court will be required to approve intelligence collection on foreign targets overseas. Last April, the Director of National Intelligence (DNI) highlighted significant intelligence gaps in foreign intelligence collection efforts and asked for a legislative solution. Due to technological advancements over the years, the structure of the 1978 FISA bill caused the Government to seek and obtain court approval before targeting a foreigner overseas despite the clear legislative intent to provide a framework for collecting foreign intelligence information within the United States. The Committee majority did nothing about the gap for months, until Republicans successfully accomplished passage of the Protect America Act in early August.[1] Now, this Committee's formal "long-term" proposed solution to this problem is to expressly inject—for the first time—a United States court into foreign intelligence collection abroad, with a two year sunset that fails entirely to provide permanent tools to the Intelligence Community.

H.R. 3773

H.R. 3773 is not the product of a bipartisan process. It does not reflect discussions between the majority and the minority, or discussions the Committee has had with the Administration. It is also important to note that the minority was not consulted on specific text before introduction of the bill, and did not receive the final text of H.R. 3773 until twenty-four hours before the markup. In the brief period we had to review the legislation before Committee consideration, we uncovered numerous, serious problems rendering this bill beyond repair.

[1] Indeed, we offered comprehensive FISA reform as an amendment to the FY '08 Intelligence Authorization bill during the Committee's markup and on the House floor in early May, which were rejected by the Democrats who instead voted to divert resources for environmental spying and wasteful earmarks. When the House failed to act, the DNI began a public campaign to underscore the worsening intelligence gap caused by FISA. Instead, the Committee remained focused on a historical review of a program that no longer exists, and subsequently canceled a FISA modernization hearing with the DNI pushing this critical issue into the fall. After sustained efforts by the Republicans, Democrats reluctantly moved a piece of legislation that was unacceptable to the DNI. After the Senate passed a bill that gave the Intelligence Community the tools it needed, the House finally passed a short-term FlSA fix on a bipartisan basis.

First, notably absent from this bill is any type of retroactive liability protection for carriers alleged to have assisted the Government following the attacks of September 11, 2001. Without this liability protection, private companies—that are alleged to have done exactly what their country asked them to—would be subjected to decades of protracted litigation. Moreover, these companies face improper claims for tens of millions of dollars in damages to scores of different plaintiffs. In addition, continued litigation on this front threatens to disclose highly classified national security information potentially exposing us to great harm from our enemies. Failing to provide retroactive liability protection to these companies jeopardizes the prospects for long-term cooperation necessary between the Intelligence Community and the private sector. Notwithstanding this, the majority has hinged this vital retroactive liability provision on a political battle with the White House over documents relating to the Terrorist Surveillance Program (TSP) described by the President, despite having reviewed relevant documents and conducted extensive interviews with former Attorney General Ashcroft and key Justice Department officials.

Second, this bill expressly requires court approval to conduct surveillance on foreign intelligence targets overseas. The bill contains a hollow statement that a court order is not required to intercept communications between non-U.S. persons that are not located within the United States that fails to consider the practical reality of intelligence collection in the 21st century. This would limit the authority to only instances where it could be reasonably determined *in advance* that a targeted person would communicate with *no* U.S. person, and would make *no* call to the United States. Therefore, simply stating that an order shall not be required when both ends of a communication are known has no practical value for our intelligence professionals in the field.

Third, the bill narrows the type of foreign intelligence that the Government can collect under the so-called "basket warrants" to include only national security foreign intelligence. This will force NSA analysts to make real-time calls as to whether they are gathering foreign intelligence for national security reasons or for other foreign affairs purposes. As we've learned from 9/11, connecting the dots is essential, and we need not be constructing new walls and creating more hoops for our intelligence professionals to jump through when collecting information that may turn out to be vital to saving lives. The original purpose behind modernizing FISA is to collect foreign intelligence from foreign targets overseas with greater efficiency, and not to create new barriers. Foreign targets located overseas have no privacy rights under U.S. laws and we should not be involving United States courts in approving warrants to collect information on them.

Fourth, H.R. 3773 would require the Intelligence Community to compile a new database to track instances where U.S. person information was incidentally acquired when surveilling foreign intelligence targets overseas, and to report on databases to Congress. We question how the civil liberties of U.S. persons are better protected by creating a new, separate database of indefinite duration to track this information. Normally, U.S. person information that does not contain foreign intelligence information would be either

expunged or age-off of NSA's databases. As such, this provision would alarmingly heighten the intrusion on the privacy of U.S. persons rather than protect it. The bill already contains extensive provisions for reporting of such instances to the Committees.

Fifth, in addition to failing to provide retroactive liability protection, this bill fails to provide any liability protection for third parties who may assist the government under an emergency authorization prior to obtaining a "basket order." Not including prospective liability protection in emergency authorizations jeopardizes long-term prospects for cooperation with private sector entities. The majority's failure to address this issue illustrates either sloppy drafting indicative of the hasty, unilateral drafting process this bill underwent, or a disregard for the essential service that third parties provide to the Intelligence Community. We assume the former is the case, but this flaw remains in the bill post-markup.

Additionally, this bill contains no provision allowing third parties asked to assist the Government to challenge orders of the FISA Court. This protection was specifically provided in the Protect American Act, and it is curious that it's left out of this bill. Again, this omission appears to be a product of hasty drafting and a failure to collaborate and seek input when drafting the text of the bill.

Sixth, we cannot support a bill that contains a sunset provision for just over two years from now. The majority provides for a sunset of these new provisions on December 31, 2009, thereby failing to provide any long-term, predictable authority and capability to the Intelligence Community or outside parties. The Administration has testified before Congress several times citing the Intelligence Community's need for a modernized FISA bill and that it lacks the tools necessary to protect the country. Our work to permanently modernize FISA now spans two congresses, and nearly two years, and the majority would have this bill expire just over two years from now. Every time the law changes in a substantive way, the Government must go through an arduous, time consuming process of implementing those changes, putting into place new procedures, and retraining personnel on those new procedures. It can take months to fully implement such substantial changes to the law. The IC has asked for a permanent solution to a fundamental problem, and this Committee has responded with a dramatically different proposal that does not meet their needs and contains a two year sunset. On this timeframe, this issue is certain to consume this Committee for the next two years, and will leave the Intelligence Community in a tenuous position. We are committed to providing permanent, effective tools to the Intelligence Community to best carry out their mission, and are disheartened to learn that the Majority is not committed to doing the same.

Seventh, the Committee also expanded the role of the FISC into foreign intelligence collection overseas. The FISC was originally created as part of a structure to conduct foreign intelligence surveillance within the United States. Section 3(e) of the RESTORE Act however, would permit judges of the FISC to modify an application for a "basket order" to conduct surveillance on *foreign* targets *foreign* countries, but contains no guidance with respect to standard of review. It is beyond us why the majority believes the appropriate role of a federal court is to oversee foreign intelligence

collection and what link this role would have to protecting civil liberties of United States persons. The responsibility for foreign intelligence collection abroad lies squarely with the President under the Constitution and overwhelming precedent of the courts.

In addition, FISC judges would be given the authority—in fact the requirement—to assess compliance with the order every 120 days—again with *no restriction* to the scope of review or remedy. This would put judges in the extraordinary position of supervising intelligence professionals or even U.S. troops overseas. Any court review of the procedures, or processes for surveillance of foreign terrorists in foreign places should allow much greater deference to our foreign intelligence officials who have the expertise and authority to conduct such surveillance. This provision, like so many others in this bill, ignores the intent behind the 1978 FISA bill, which was not to hinder foreign intelligence gathering, but rather to provide a framework for intelligence gathering in the United States.

Eighth, the Committee imposes a burdensome auditing requirement on the Intelligence Community and the Department of Justice Inspector General (DOJ IG). This provision requires the DOJ IG to audit compliance with the procedures in 105B every 120 days. Not only is this incredibly burdensome, but it is nonsensical to require non-intelligence personnel (the DOJ IG) to perform an audit of Intelligence Community professionals. The NSA has an independent Inspector General that would be the more appropriate body to conduct audits on the NSA.

Ninth, the bill seeks additional investigation into the Terrorist Surveillance Program, which is no longer in existence. Section seven of the bill requires the DOJ IG to perform an audit of TSP, and a section newly added during markup would require the President to fully inform the Intelligence committees on TSP. An audit by the DOJ IG would, once again, impose non-Intelligence Community personnel into the work of the Intelligence Community. More significantly, the DOJ IG auditing provision is of questionable constitutionality, as it would require an executive branch agency to audit the conduct of the President. It also requires the President, a classifying authority, to grant access to extremely sensitive information, and requires the IG to acquire and produce documents containing legal advice given to the President by his lawyers.

More importantly, we remain baffled by the majority's continued contention that it has not been fully informed by the Executive Branch on these sensitive intelligence matters. Democratic Committee members have been fully and extensively briefed on TSP, as has the current Speaker of the House, since its inception. In addition, just four months ago this Committee conducted an extensive, comprehensive historical review of TSP. This Committee has interviewed or heard testimony from many current and former senior DOJ, NSA, and ODNI officials and has reviewed countless documents in connection with these activities. In addition, the Committee received briefings on the legal foundation for TSP and has available an unclassified, 42 page white-paper from the Department of Justice detailing the legal basis for TSP, entitled "Legal Authorities Supporting the Activities of the National Security Agency Described by the President." It is disingenuous and misleading to the American people for the majority to contend that it

has not been fully briefed about these classified NSA surveillance activities. The DOJ IG audit provision is, essentially, an end run around the traditional mechanisms for seeking documents from the Executive Branch. The Committee has been negotiating with the White House on outstanding document requests, and the United States Code is not the appropriate place to air these disputes.

Both of the aforementioned DOJ IG audits, as well as other reporting requirements in this bill would be provided jointly to the Judiciary Committees. The Rules of the House provide exclusive jurisdiction over intelligence sources and methods to the Committee. To the extent that these reporting requirements contemplate providing materials containing sources and methods, these provisions are inconsistent with the House Rules. We remain committed to preserving this Committee's jurisdiction under the Rules of the House, and are similarly discouraged that the majority is not.

Finally, Section 10 restates the existing statutory provision that FISA is the exclusive means for conducting electronic surveillance for the purpose of gathering foreign intelligence information. The exclusivity provision is superfluous and arguably could constitute an unconstitutional infringement of the President's constitutional authority. The bill also contains a provision purporting to require a specific statutory authorization to conduct electronic surveillance that may be subject to constitutional challenge. The President's constitutional authority to take such measures he deems necessary to protect the Nation from potential future attacks or hostile acts of a foreign power cannot be limited by simply restating a statutory provision. By repeating a provision that it knows is already contained in FISA, and is of questionable constitutionality, the majority insists on focusing this debate on the past and not the present need to permanently modernize FISA. Our focus should be on modernizing FISA and giving the Intelligence Community the tools they need to protect this country, and not on partisan political rhetoric concerning a program that no longer exists.

THE PROTECT AMERICA ACT

We offered a substitute amendment, which would have made PAA permanent and provided retroactive liability protection to third parties alleged to have assisted the Government following the attacks on September 11, 2001, that was summarily rejected by the majority citing the now debunked "parade of horribles." The PAA represented a strong bipartisan consensus that was supported by forty-one Democrats in August and gave the Intelligence Community the tools it needed.

The Administration has been implementing PAA with extraordinary transparency to this Committee. Staff and Members have been briefed several times, including at the NSA, have received copies of relevant documents, and have heard testimony from Administration officials in both closed and open session.

The Committee specifically asked Administration witnesses to put into writing their views about the reach of this bill and the concerns that had been raised. In a letter, dated September 14, 2007, from Assistant Attorney General Kenneth L. Wainstein, the Justice Department made a rare, public written statement rebuking the "parade of horribles" that the majority cited and delin-

eating how the Executive Branch will interpret the law. Specifically, Mr. Wainstein stated that these hypotheticals are inconsistent with a plain reading of the entire FISA statute and that:

- The PAA leaves undisturbed FISA's definition of electronic surveillance as it applies to domestic-to-domestic communications and surveillance targeting persons located in the United States, and that the Executive Branch will not use the PAA to "target" a person in the U.S. by seeking foreign information "concerning" a person abroad.
- The Executive Branch will not use the PAA to conduct physical searches of the homes or effects of Americans, including physical searches of U.S. mail, U.S. homes or businesses of foreign intelligence targets outside the U.S., and personal computers or hard drives of individuals in the U.S. without a court order.
- That the Executive Branch will not use PAA to reverse target U.S. persons inside the United States, as doing so would be a violation of FISA.
- That 105B of PAA does not authorize the collection of, for example, of medical or library records for foreign intelligence purposes and that the Executive Branch will not use this authority to obtain business records of individuals located in the U.S. on the theory that they "concern" persons outside the U.S.

Further, the Administration has repeatedly expressed its willingness to consider language from the Committee that would clarify or narrow language in the PAA to address these perceived ambiguities. Notwithstanding such transparency, and willingness to clarify the bill, this Committee passed a bill that essentially takes three steps back following our one, big step forward in enacting the PAA. This committee has not raised any specific concerns with actual implementation and, to the contrary has been continually reassured by those implementing the bill. With all of the questions and concerns addressed, the majority instead reverted to an ill-conceived partisan bill.

Continuation of the PAA ensures that the IC will not go dark against terrorists, that we don't give radical jihadists greater rights than those afforded to Americans in court ordered surveillance in criminal cases, and that we have a permanent solution to the intelligence gaps that we potentially face. The House should act immediately to accomplish these goals.

PETER HOEKSTRA.
TERRY EVERETT.
ELTON GALLEGLY.
HEATHER WILSON.
MAC THORNBERRY.
JOHN MCHUGH.
TODD TIAHRT.
MIKE ROGERS.
DARRELL ISSA.

○