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

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. CONYERS, from the Committee on the Judiciary, submitted the following

R E P O R T

together with

DISSENTING VIEWS

[To accompany H.R. 3773]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, 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.

CONTENTS

69–006

THE AMENDMENT

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 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 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 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 judge shall 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 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) a copy of the application, including the certification made under section 105B(b)(1); and

"(B) a description of the primary purpose of the acquisition for which the application is submitted; 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 in-

clude 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. 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 December 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. 8. 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 Com-

mittee 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. 9. 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 7; and

(3) the record-keeping system and reporting requirements under section 8.

SEC. 10. REITERATION OF FISA AS THE EXCLUSIVE MEANS BY WHICH ELECTRONIC SURVEILLANCE MAY BE CONDUCTED FOR GATHERING FOREIGN INTELLIGENCE INFORMATION.

(a) EXCLUSIVE MEANS.—Notwithstanding any other provision of law, the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which electronic surveillance may be conducted for the purpose of gathering foreign intelligence information.

(b) SPECIFIC AUTHORIZATION REQUIRED FOR EXCEPTION.—Subsection (a) shall apply until specific statutory authorization for electronic surveillance, other than as an amendment to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), is enacted. Such specific statutory authorization shall be the only exception to subsection (a).

SEC. 11. 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. 12. 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 AND SUMMARY

H.R. 3773, the "Responsible Electronic Surveillance That is Overseen, Reviewed, and Effective Act of 2007" (RESTORE Act of 2007) would provide a mechanism, through December 2009, to conduct foreign electronic surveillance for the purpose of defense against terrorism and other national security threats, without the need for individual warrants for overseas targets, while protecting the civil liberties of Americans whose communications may be intercepted in the process. It would also require increased accountability through data collection, auditing, and mandatory reporting to Congress. And it would provide additional resources for the National Security Agency and Department of Justice to ensure that there are no backlogs of critical intelligence gathering.

Importantly, it removes any "foreign-to-foreign" ambiguity by making it clear that purely foreign communications do not require a court order even when they transit the U.S. or the acquisition is in the United States as a result of changes in communications technology since FISA was first enacted. Through this approach, the RESTORE Act specifically prevents the extension of any Fourth Amendment or statutory protections to overseas targets such as Osama Bin Laden or other members of terrorist organizations.

BACKGROUND AND NEED FOR THE LEGISLATION

On August 5, 2007 the President signed into law the "Protect America Act"[1] ("PAA"), which enacted short-term revisions to the Foreign Intelligence Surveillance Act[2] ("FISA") and exempted large

[1] Pub. L. No. 110–55.
[2] 50 U.S.C. § 1801 et seq.

portions of foreign intelligence surveillance from court review. Section 6 of the PAA provides that it sunsets in February 2008. The RESTORE Act replaces the PAA, extending the ability of the government to acquire communications of persons abroad for the purpose of terrorism and other national security threats, but in a manner that responds to concerns that the PAA lacked sufficient judicial safeguards for Americans' phone calls, e-mails, and other communications.

The Foreign Intelligence Surveillance Act and Protect America Act Enacted in 1978 in the wake of revelations of widespread intelligence-gathering abuses, FISA established the exclusive means by which the Government conducts surveillance of Americans [3] for the purpose of gathering foreign intelligence. Under FISA as structured before the Protect America Act altered it (hereinafter, "traditional FISA"), the Government typically must seek an order from the FISA court before conducting electronic surveillance of Americans for foreign intelligence information. This order is sometimes referred to as a FISA "warrant."

THE "TERRORIST SURVEILLANCE PROGRAM"

Since September 11, 2001, the Administration has engaged in various warrantless surveillance programs. Following revelations of the existence of such programs in 2005,[4] the President has admitted to at least portions of the programs, sometimes referred to as the Terrorist Surveillance Program ("TSP") [5]. An oversight hearing into these programs was held by the Subcommittee on the Constitution. Civil Rights and Civil Liberties on June 7, 2007. Additional revelations about these surveillance programs have been obtained through the congressional oversight of U.S. Attorney firings and related Committee oversight of the Justice Department. The Administration turned to an extra-legal surveillance program despite emergency procedures available under existing law and the fact that it is incredibly rare for the FISA Court to ever turn down a request for a warrant.[6]

The Administration has acknowledged that, in carrying out its post-9/11 surveillance programs, it did not completely meet the then-existing FISA requirements. The Department of Justice has explained to Congress that "FISA could not have provided the speed and agility required for the early warning detection system." [7] The Administration argues that the NSA program did not

---

[3] FISA defines the term "United States persons" to include not only American citizens, but lawfully admitted aliens and other narrow classes. See 18 U.S.C. § 1801(i).

[4] James Risen and Eric Liehtblau, "Bush Lets U.S. Spy on Callers Without Courts" New York Times, December 16, 2005 at A1.

[5] President Bush's Radio Address, Dec. 17, 2005, available at *http://www/whitehouse.gov.news/releases/2005/12/20051217.html*). The term "terrorist surveillance program" was used by then-Attorney General Gonzalez in February 2006. See Prepared Statement of Hon. Alberto R. Gonzales, Attorney General of the United States, available at *http://www.usdoj.gov/ag/speeches/2006/ag*_speech_060206.html. In an August 2007 letter, Attorney General Gonzales stated, "[B]efore December 2005, the term 'Terrorist Surveillance Program' was not used to refer to these activities, collectively or otherwise. It was only in early 2006, as part of the public debate that followed the unauthorized disclosure and the President's acknowledgment of one aspect of the NSA activities, that the term Terrorist Surveillance Program was first used." Letter from Attorney General Alberto Gonzales to Senator Patrick J. Leahy, August 1, 2007 (letter on file with the House Judiciary Committee).

[6] Spy Court Rejects No Requests in 2006, CNN.Com, May 1, 2007, available at *http://www.cnn.com/2007/POLITICS/05/01/01/fisa.court*.

[7] Letter from the Honorable William E. Moschella, Assistant Attorney General, to the Honorable Pat Roberts, Chairman, Senate Select Committee on Intelligence, the Honorable John D.

Continued

violate existing law because Congress implicitly authorized such a program when it enacted the Authorization for the Use of Military Force (AUMF).[8] Since January 10, 2007, according to a letter from Attorney General Gonzales, the TSP was conducted pursuant to review by the FISA Court.[9]

THE "PROTECT AMERICA ACT"

In late July 2007, the Administration called on Congress to complete short-term FISA revisions before its summer recess in August, to close what it termed pressing gaps in the surveillance regime. Director of National Intelligence J. Michael McConnell publicly characterized these gaps as having been created by different rulings concerning the surveillance program by different judges of the FISA Court after the program was brought under the Court's supervision in January 2007, leaving the intelligence community "in extremis" after May 31, 2007.[10]

The PAA modified FISA's definitions of electronic surveillance to exclude from FISA Court oversight situations where the underlying premise is that the surveillance is "directed at a person reasonably believed to be located outside of the United States."[11] This was put forward by the Administration as a means to address the "foreign-to-foreign" problem, as to which there is consensus that purely foreign communications are properly outside of the scope of FISA. This mechanism also had the effect of removing protections for "United States persons'" communications. For instance, the required minimization procedures and restrictions on dissemination

---

Rockefeller, IV, Vice Chairman, Senate Select Committee on Intelligence, the Honorable Peter Hoekstra, Chairman, Permanent Select Committee on Intelligence, and the Honorable Jane Harman, Ranking Minority Member, Permanent Select Committee on Intelligence (December 22, 2005) (on file with the U.S. Senate Select Committee on Intelligence) (hereinafter "Moschella letter").

[8] Id.; Authorization for the Use of Military Force, Pub. L. No. 107–40, 115 Stat. 224 (2001). In a press conference in December 2005, then-Attorney General Gonzalez was asked why the Administration did not seek legislation for the surveillance program:

"Q. [Reporter]: If FISA didn't work, why didn't you seek a new statute that allowed something like this legally?

ATTORNEY GENERAL GONZALES: That question was asked earlier. We've had discussions with members of Congress, certain members of Congress, about whether or not we could get an amendment to FISA, and we were advised that that was not likely to be—that was not something we could likely get, certainly now without jeopardizing the existence of the program, and therefore, killing the program. And that—and so a decision was made that because we felt that the authorities were there, that we should continue moving forward with this program."

Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy for National Intelligence, Dec. 19, 2005, available at *http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html.* Thus, the Administration argued on the one hand that Congress authorized the NSA program in the AUMF, and at the same time, asserted that it did not ask Congress for such authorization because it feared Congress would not grant such authorization. Moreover, Congress specifically rejected the Administration's request that the AUMF give President authority "to deter and pre-empt any future acts of terrorism or aggression against the United States." See CRS Report RS 22357, Authorization for Use of Military Force in response to the 9/11 Attack (P.L. 107–40); Legislative History, by Richard F. Grimmett, available at *http://www.congress.gov/erp/rs/pdf/RS22357.pdf.*

[9] The Administration has refused to permit full House or Senate Judiciary Committee access to the FISA court orders and other details under which the program has been conducted, despite ongoing requests for information. The Administration has also refused to indicate whether it has conducted other programs of warrantless communication interceptions or physical searches, and whether any are currently continuing.

[10] Chris Roberts, Debate on the Foreign Intelligence Surveillance Act (transcript of interview with Director of National Intelligence Mike McConnell), available at *http://www.elpasotimes.com/news/ci*—6685679. *See also* Carol D. Leonnig and Ellen Nakashima, Ruling Limited Spying Efforts: Move to Amend FISA Sparked by Judge's Decision, Wash. Post, August 3, 2007, at A1 (concerning revelations of Court action by Minority Leader John Boehner).

[11] 50 U.S.C. 1805A (2007).

in FISA only apply to electronic surveillance as set forth in Section 101(f) of FISA.

Having re-defined electronic surveillance to exclude any such types of collection, the PAA set up mechanisms by which the Executive Branch, without court review, could issue its own year-long administrative program authorizations to obtain "foreign intelligence information from or with the assistance of a communications service provider [or its custodian]"[12] that "concern" a person outside of the United States. While the contents of the international communication sought had to "concern" a person outside of the United States, the PAA was ambiguous and could be interpreted as permitting the target of the interception to be an American citizen inside the United States.

As a precondition for issuing its administrative authorization under the PAA, the Executive Branch is required to certify to itself that: (1) there are reasonable procedures in place for determining that the information concerns a person outside of the United States; (2) the collection is not otherwise defined as electronic surveillance under FISA; (3) the information is gathered from a communications company, custodian, or other person in control of the communication or record; (4) a significant purpose of the acquisition is gathering foreign intelligence information; and (5) the minimization procedures under FISA apply.[13]

Under the PAA, the Executive Branch must submit a copy of these administrative authorizations to the FISA Court, but the authorization is sealed and is not reviewed by the FISA Court unless and until it is challenged by an entity that has received such an order.[14] Under the PAA, the government may direct a communications company or other custodian to allow immediate access to its facilities for collection.[15] The Administration has publicly stated its view that this does apply to libraries or medical facilities, but has conceded that it might be read to include business records. Nevertheless, the Administration claims that it would not use the authority with respect to these types of information.[16] If the entity refuses to allow immediate access, the Government may seek a contempt ruling from the FISA Court. Review of challenges by the FISA Court, the Foreign Intelligence Surveillance Court of Review (FISCR), and even the Supreme Court is confined to determining whether "such directive does not meet the requirements of [of FISA as amended by the PAA] or is otherwise unlawful."[17]

The PAA provided prospective immunity for entities that comply with Government requests for assistance in carrying out these new surveillance activities.[18] This is consistent with pre-existing law that provides immunity so long as the entity is acting in response to a statutorily sanctioned government request. The PAA did not provide retroactive immunity for actions taken pre-PAA without certifications reflecting an order of the FISA Court.

---

[12] 50 U.S.C. 1805B(3) (2007).
[13] 50 U.S.C. 1805B (2007).
[14] Id.
[15] Id.
[16] Letter of Assistant Attorney General Kenneth Wainstein to HPSCI Chairman Sylvestre Reyes, Sept. 14, 2007, at 4.
[17] 50 U.S.C. 1805B (2007).
[18] Id.

The PAA does authorize some limited judicial and Congressional oversight, with procedures in which the certifications are filed post hoc with the FISA Court, and a requirement that the Government inform the Intelligence and Judiciary Committees whether the Executive Branch is complying with its own minimization procedures.[19] The Executive Branch must submit to the FISA Court the procedures by which this new surveillance program will "not constitute electronic surveillance" (in other words, will be directed at targets or facilities overseas) within four months of enactment, and then annually after that.[20] The FISA Court is directed to determine by February 2008 whether the procedures provided by the Government are reasonably designed to ensure that acquisitions of communications are directed at people overseas. Even this minimal level of review is to be judged only on a "clearly erroneous" standard.[21]

H.R. 3773, THE RESTORE ACT

The RESTORE Act provides a flexible program of surveillance against terrorists and other security threats. In circumstances where such surveillance is reasonably likely to encompass the interception of Americans' communications, the RESTORE Act requires that such surveillance be conducted under rules reviewed and approved by the FISA Court, and further requires that traditional FISA warrants be obtained when the government seeks to conduct surveillance against persons reasonably believed to be in the United States. Moreover, RESTORE provides ongoing oversight and enforcement by the FISA Court, the DOJ Inspector General, and the Congress.

Section 10 of the RESTORE Act firmly reiterates that FISA is the exclusive means of foreign intelligence surveillance that may involve the interception of the communications of American citizens. The Act mandates that FISA exceptions can only be established through explicit statutory authorization.

Programmatic authorizations to target terrorist groups and other foreign threats while ensuring safeguards for Americans who may be intercepted in the process

The RESTORE Act strengthens American counterterrorism efforts and Constitutional liberties at the same time. For a truly effective foreign intelligence surveillance effort, we must have certainty, legality, and flexibility. The RESTORE Act strikes that balance.

To solve the confusion over whether the intelligence community must obtain individualized warrants against foreign targets when there is a risk that they might be talking with Americans, now that many communications transit the United States and can be acquired here, the RESTORE Act would allow a program of collection against the target organization or group (a "foreign power," as defined in Section 101(a) of FISA), upon application and review. Thereafter, rather than having to obtain individual warrants against *particular* foreign persons, the government will be able to incorporate them into their targeting of that group.

[19] 50 U.S.C. 1805C (2007).
[20] Id.
[21] Id.

The Committee emphasizes that the Act does not require the Government to obtain individual warrants for terrorists overseas. Rather, this is a method by which to guarantee that the Administration can effectively target and surveil foreign terrorists without a warrant while preserving and protecting the rights of Americans' whose conversations may be intercepted.

In light of the fact that such a programmatic authorization is a new approach, the RESTORE Act sets forth streamlined application procedures to guard against overbreadth or abuses while providing the additional flexibility. Section 3 of the RESTORE Act requires the Attorney General and Director of National Intelligence to apply to the FISA Court for an order authorizing the surveillance program described in the certification. The FISA Court must then issue a judicial directive to the communications provider to assist the government. Under this approach, the intelligence community is not required to obtain individual warrants when foreign communications are targeted, even if it is reasonably foreseeable that some of those communications may involve Americans. Nevertheless, the Court does have an oversight role when it is reasonably foreseeable that Americans' communications will be intercepted. Thus, Americans' privacy rights are appropriately protected, and the telecommunications providers have the certainty that they are being asked to provide information only as part of a legal process.

The role of the court in the RESTORE Act's Programmatic Authorizations of Foreign Communications

Unlike the PAA, the RESTORE Act provides for court involvement from the outset. As noted, the Executive Branch cannot simply undertake surveillance on its own where it is reasonable that Americans' communications may be intercepted, but must first obtain FISA Court authorization. Under section 3 of the RESTORE Act, before issuing the authority, the Court must review and approve: (1) procedures for determining that the surveillance target is outside the United States; (2) guidelines to ensure individual FISA warrants are obtained if surveillance begins to target Americans; and (3) procedures to ensure that collected information is "minimized" to protect Americans' legitimate privacy interests. The FISA Court reviews all of these procedures to determine whether they are reasonably designed to achieve these goals.

Notably, the FISA Court is not required to make any probable cause findings, or any other findings as to the evidentiary basis, reasonableness, or appropriateness of such surveillance those determinations are made in the Executive Branch. The Court's role is to appropriately safeguard the rights of Americans.

In contrast, the PAA only allows Court review of general procedures for determining that the target is abroad and, even then, limits the Court to a "clearly erroneous" standard of review, tantamount to a rubber stamp.[22] Under section 3 of the RESTORE Act, however, the FISA Court has an ongoing role in determining the reasonableness of its authorizations and must assess compliance with the procedures that it has initially approved.

Collectively these judicial responsibilities still permit programmatic surveillance based on certifications by the Attorney

[22] 50 U.S.C. 1805C (2007).

General and the Director of National Intelligence. But without these improvements, this new system of communications surveillance which could potentially violate the legitimate privacy rights of countless innocent Americans would remain entirely in the hands of Executive Branch officials. Recent and past history amply demonstrate that such concentration of unchecked power poses unacceptable threats to our civil liberties. For instance, that collecting and processing vast amounts of information about Americans is prone to error;[23] and that investigative techniques employed without adequate judicial oversight can lead to substantial abuse.[24] Adequate minimization rules are important for ensuring that the NSA can collect appropriate intelligence without it being indiscriminately disseminated throughout the Government.[25] This is a particular concern regarding the broader authorization set forth in Section 105B of the PAA, which bypasses FISA review entirely and relies on internal agency procedures and minimization as the only line of defense of Americans' privacy.

Strengthening the role of the FISA Court will not result in judges second-guessing intelligence experts; nor will it burden the intelligence community's ability to obtain vital intelligence promptly and use it effectively. The FISA Court will not second-guess intelligence judgments of who should be targeted, what information should be sought, or how it can be accessed within the United States. The bill leaves intelligence analysis to the intelligence professionals. The FISA Court will oversee the procedures by which the intelligence community determines that targets are indeed foreign nationals, and to ensure that minimization takes place appropriately and that individual FISA warrants are obtained when necessary.

That is a fitting role for the courts in a society based on the rule of law; appropriate court involvement should be welcomed and respected.

The FISA Court process set forth in the bill will not overburden the intelligence community. Emergency provisions in section 4 of the bill will ensure that no legitimate target goes uncovered. Moreover, the FISA Court's approvals of the Attorney General's procedures, and the guidelines required by the bill, are expected to be standardized in all but the most unusual cases. Moreover, as noted below, section 9 of the bill authorizes sufficient additional personnel and funding resources to ensure that neither the certification process nor the oversight audits of the program will slow

---

[23] *See* Julia Preston, "*Judge Blocks Bush Measure on Illegal Workers,*" NEW YORK TIMES, October 11, 2007 at A1 (Court halts immigration employment enforcement program because Social Security database "was laden with errors not related to a worker's immigration status" that would result in up to 12.7 million Americans being misidentified as illegal aliens).

[24] Office of Inspector General, U.S. Dept. of Justice, A Review of the Federal Bureau of Investigation's Use of National Security Letters, Mar. 2007.

[25] The minimization rules generally required the "masking" of the identities of the U.S. persons on the summaries of the intercepted phone calls, though the information as to the identity may be disclosed upon request by to other components of the government. The New York Times reported that such disclosures were made to former Stated Department official John Bolton directly, and bluntly raised the specter that such disclosures could be made for political purposes: "If the National Security Agency provides officials with the identities of Americans on its tapes, what is the use of making secret those names in the first place? More troubling still is the apparent lack of guidelines or controls on this process: the whole thing seems like an invitation to any Beltway Richelieu hoping to gain an edge on his political foes." Patrick Radden Keefe, *Big Brother and the Bureaucrats*, N.Y. Times, Aug. 10, 2005, *available at* http://query.nytimes.com/gst/fullpage.html? res= 9F04E4DF 143EF933A 2575BC0A 9639C8B63&n= Top%2FReference%2 FTimes%20 Topics%2F Organizations%2FU%2F United%20Nations%20

down or backlog America's acquisition and use of critical intelligence. Rather, by requiring that the applications identify the foreign power against whom acquisition is directed, the bill will ensure that the authorizations do not give the Government an unlimited "blank check" to conduct surveillance against anyone in the United States, but will instead focus surveillance on the particular threat to our Nation. Such a reasonable requirement guards against the "drift-net" collection of all communications world-wide, and protects against the targeting of innocent groups.

Because warrants are not required for the programmatic surveillance authorization set forth in section 105B of FISA as revised by the bill, the bill adds other provisions to the PAA regime in order to safeguard the legitimate privacy interests of innocent Americans. Without these improvements, foreign intelligence can all too easily become domestic surveillance. These improvements ensure that when the Executive Branch is engaging in activities that involve the reasonable likelihood of the interceptions of conversations of United States persons, the judiciary may examine those activities to ensure that they do not transgress constitutional and statutory boundaries. It is important to note that none of these provisions prevent the intelligence community from listening to international communications, whether of Osama Bin Laden himself, other members of al Qaeda, or less notorious targets. It merely means that appropriate safeguards will apply where warranted.

Protecting Americans at home and abroad

While Section 105(a) excludes from the warrant requirement the interception of communications among participants who are all outside the United States, that exclusion applies only to communications whose participants are not "United States persons" as defined in Section 101(I) of FISA—that is, who are not U.S. citizens or aliens lawfully admitted for permanent residence. Accordingly, this provision does not extend any protections to illegal aliens or aliens who are in the United States on a non-immigrant visa. It does provide appropriate protections to Americans and certain legal aliens in keeping with fundamental Constitutional principles.

The courts generally have held that the Constitution, including the Fourth Amendment, protects United States persons abroad.[26] At a time when it is now easy to obtain communications in the United States, given the growing interconnectedness of communications technologies, the Committee does not believe that Americans should lose their Fourth Amendment protections when traveling abroad. The PAA's overbreadth would allow unfettered access to Americans' communications whenever they set foot outside the country or leave its shores.

[26] Courts which have examined this point are generally in agreement that the Fourth Amendment protects U.S. persons from search abroad by their government. See, e.g. United States v. Conroy, 589 F2d. 1258, 1264 (5th Cir. 1979); Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144, 157 (D.D.C. 1976). It has been suggested that this warrant requirement may not apply when the interception is accomplished abroad, because in that case the search may otherwise be reasonable. In judging the "reasonableness" of the search, however, the location of the intercept can be as important as the location of the U.S. person under surveillance. See, e.g., United States v. Verdugo-Urquidez, 494 U.S. 259, 278 (1990) (Kennedy J. concurring) ("The absence of local judges available to issue warrants, the different and perhaps unascertainable conceptions of reasonableness and privacy that prevail abroad, and the need to cooperate with local foreign officials all indicate that the Fourth Amendment warrant requirement should not apply in Mexico as it does in this country.").

Section 3 of the RESTORE Act protects the privacy of all Americans abroad by mandating that the programmatic authority of Section 105B of FISA can only be used where "the targets of the acquisition are reasonably believed to be [non-United States persons]." In addition, the Executive Branch must certify in the application that it has promulgated guidelines to ensure that if surveillance becomes directed at someone reasonably believed to be a United States person, then a traditional FISA warrant is obtained as required by law.

There have been published reports about the intelligence and law enforcement communities having telecommunications companies assist in the analysis of the "social networks" with data about suspects' patterns of communication. Like ripples in a pond, network analysis can lead to new subjects whose communications can then be targeted.[27] Following such leads is an important and legitimate investigative tool, and the RESTORE Act does not prohibit this activity. The bill mandates safeguards to prevent abuses stemming from such use, by requiring that a warrant once a substantial purpose of the acquisition is to acquire the communications of a United States person. This requirement is fully consistent with Director of National Intelligence McConnell's insistence that NSA will not target an American in the United States without a FISA warrant. The FISA Court will approve the guidelines if it concludes that they are reasonably designed to ensure such an outcome.

As noted above, section 2 of the RESTORE Act settles the issue of "foreign-to-foreign" communications, making clear that purely foreign communications do not require a FISA warrant and that foreign targets abroad are not to be extended Constitutional protections. Unlike the PAA, however, the RESTORE Act does not accomplish this by exempting such acquisitions from FISA's definitions of electronic surveillance. That approach has undercut other vital aspects of FISA that ensured that law-abiding Americans had legal protection against inappropriate acquisition and distribution of their private communications.

Preserving the programmatic collection of terrorist information while protecting against the overbreadth of the Protect America Act

The PAA is overbroad as to the scope of information that can be sought without a warrant, and as to the nature of the sources from which that information can be demanded by the Government. The RESTORE Act removes these overbroad authorities, which the Administration has in part disavowed any intention of seeking.

For example, section 2 of the PAA authorizes the acquisition of information from domestic communications or other files and records, as long as their content concerns a person abroad, who need not even be a foreign intelligence target. Though the Administration insists that the intent of that provision is only to access the contents of the communication by the targeted person abroad, as the PAA is written the communication could be an entirely domes-

[27] *See e.g.,* Leslie Cauley, NSA Has Massive Database of Americans' Phone Calls, USA TODAY, May 11, 2006 (telephone companies cooperating with NSA pattern analysis without FISA warrants); *and* Eric Lichtblau, F.B.I. Data Mining Reached Beyond Initial Targets, N.Y. TIMES, September 9, 2007 (FBI sought "community of interest data" through National Security Letters).

tic one. Section 3 of the RESTORE Act accomplishes the objective that the intelligence community seeks, but without being so broad as to allow the warrantless tapping of Americans' mere conversations about foreigners. The RESTORE Act provides that collection under section 105B of FISA is only authorized where the target is believed to be a non-U.S. person outside of the United States and a significant purpose of the acquisition is to obtain foreign intelligence information relating to national security.

An additional overbreadth concern is raised by the PAA provisions governing whom the Executive Branch can force to turn over the information sought. Under the PAA, the Attorney General and DNI could (without a court order) demand assistance not only from communication service providers and related entities, but also from any other person or entity who has custody of or access to communications, as they are transmitted or while they are being stored.[28] Under the PAA, the Government could demand without a warrant access to any American's financial, medical, business or other private records that might contain a transcript, summary of, or notes about a communication concerning someone abroad, and could acquire these records from any custodian of records, such as a hospital or a business, or a library where the targeted person used the computer.[29] This broad scope of collection is not allowed under the RESTORE Act. In this regard, the Committee emphasizes that it does not intend for a library to be considered a telecommunications service provider for purposes of the authorities set forth in sections 105B and 105C.

Under the PAA, the Executive Branch must certify to itself that a substantial purpose of the surveillance is the acquisition of "foreign intelligence."[30] Under FISA, however, this term is defined so broadly that it would include almost any information relating to the foreign, economic, and diplomatic interests of the United States.[31] Used in this manner, the breadth of this category is stunning, with no relation to the counterterrorism emergencies evoked by the Director of National Intelligence and the President in its defense.

In response to these concerns, the RESTORE Act requires the Government, for purposes of surveillance based on programmatic authorizations under Section 105B rather than on a regular FISA warrant, to certify to the FISA Court that a substantial purpose of the surveillance will be the acquisition of foreign intelligence relating to terrorism, national defense, or other national security matters, as delineated in paragraphs (1) and (2)(A) of section 101(e) of FISA. Targets of this surveillance include radical jihadist groups, nuclear proliferators, hostile foreign governments, and narco-terrorists, among other threats.

Oversight and review

Section 3 of the RESTORE Act directs the FISA Court to conduct ongoing review of compliance with the procedures that it has authorized. Section 7 of the bill also requires vigorous audits by the independent Department of Justice Inspector General. These audits

[28] 50 U.S.C. 1805B (2007).
[29] Id.
[30] Id.
[31] 50 U.S.C. 1801(e) (1978).

are not just internal to the Department of Justice, but must be delivered to the relevant committees of Congress and the FISA Court. The audits will assess compliance with the law and how the law is working in practice, so that Congress can strengthen the foreign intelligence gathering regime further as warranted to counter foreign threats and protect Americans lives and liberties. The audits will include whether any targets were found to be in the United States; the number of Americans whose communications were acquired; any situations in which information on Americans was disseminated, and the number of FISA warrants sought based on the authorizations. The audits must be submitted to the House and Senate Judiciary and Intelligence Committees.

The Inspector General of the Justice Department has a singular record of careful, balanced, and thorough reviews of complex and controversial foreign intelligence collection programs. The audit mandated by the RESTORE Act involves judging compliance with procedures and guidelines mandated by statute, as well assessing the impact of those laws on civil liberties. Attorneys from the Department of Justice, rather than staff from the NSA, are the appropriate personnel to perform that important task, although it is expected that they can and will call on the NSA to provide data and technical expertise to complete some of that assessment.

Under section 5 of the RESTORE Act, the Justice Department Inspector General is also directed to obtain and provide to Congress critical documents concerning the Administration's extralegal warrantless wiretapping programs that have been conducted since September 11, 2001. This mandate supplements the following letter requests from the Judiciary Committee to the Administration:

- January 19 and February 1, 2007, for a classified briefing for the entire House Judiciary Committee on these programs, including the contents of January 2007 Foreign Intelligence Surveillance Court orders;
- May 17, 2007, requesting information about the Terrorist Surveillance Program and aspects of the Justice Department's involvement therein;
- July 30, 2007, reiterating prior requests and inquiring into a seemingly previously unrevealed program of surveillance;
- September 12, 2007, reiterating previous letters joining in the request for information subpoenaed by the Senate Judiciary Committee, and posing additional questions concerning, inter alia, telecommunications companies' involvement in the TSP.

As of the filing of this report, the Administration has failed to respond to any of these requests for information.

The RESTORE Act requires that the issuance of security clearances to conduct the Inspector General review is to be expedited, to avoid a repeat of the Justice Department's attempt to conduct an internal investigation into the TSP, an effort which was opened on January 11, 2006 and closed approximately three months later after the President denied Office of Professional Responsibility investigators the necessary security clearances.[32]

[32] In a March 22, 2007 letter, the Department of Justice stated: "Within the Department of Justice, [the Office of Professional Responsibility] sought assistance in obtaining security clear-

Section 5 of the RESTORE Act requires the Attorney General and DNI to submit to Congress periodic reports on acquisitions made under this certification process and on any noncompliance with procedures and guidelines in their respective agencies. Having both agencies report will enable Congress to determine whether the statute or procedures implement in need to be modified. The RESTORE Act will also establish a record-keeping system to track the volume of personal information about U.S. persons acquired under this surveillance authorization and disseminated within the Government.

The Committee believes these provisions constitute a coherent, sensible system to monitor how key provisions work in practice, in order to assess compliance with them and, equally important, to determine whether any of them need to be adjusted. This is necessary in order for Congress to perform its constitutional oversight responsibilities as a co-equal branch of Government. The oversight audits and reports should not slow down or backlog acquisition and use of critical intelligence, as the bill authorizes sufficient additional personnel and other resources to offset any increased workload involved in complying.

Sunset provisions

The RESTORE Act sunsets in December 2009, to encourage assessment and appropriate modification in light of ongoing oversight by both the Judiciary and Intelligence Committees. The PAA was passed without hearings or meaningful legislative history, such as committee reports. After several hearings, extensive debate within Congress and among the public, and further analysis of that law, it is now clearer the extent to which the PAA could open the way for the invasion of privacy of innocent American families and businesses and thereby raise serious constitutional concerns. These flaws require Congress to act before the PAA's mandated sunset in 2008.

Moreover, the experience with the PAA demonstrates why passing a permanent law at this juncture would be unwise. The Executive Branch has still not provided Congress with critical information about past surveillance programs and problems. While H.R. 3773 is a vast improvement, and responsibly addresses shortcomings and problems in both FISA and the PAA as they are currently understood, continued monitoring will be necessary as to how it is implemented and its impact on core civil liberties. The RESTORE Act creates a very thorough monitoring system that will help provide sufficient information for effective oversight. The Act will sunset in December 2009, allowing sufficient time for a comprehensive assessment of both these revisions and PATRIOT Act to be undertaken.

---

ances to the Terrorist Surveillance Program to conduct its investigation. This request reached the Attorney General . . . The Attorney General recommend to the President that OPR be granted security clearances to the Terrorist Surveillance Program. The President made the decision not to grant the requested security clearances." Letter from Richard A. Hertling, Acting Assistant Attorney General, to Rep. John Conyers, Jr., Mar. 22, 2007 (letter on file with House Committee on the Judiciary).

HEARINGS

The Committee held two days of hearings on the effects of the Protect America Act. On September 5, 2007, testimony was received from: Bob Barr, former Member of the House of Representatives (R–GA), and currently a member of the Liberty and Security Initiative of the Constitution Project; Suzanne Spaulding, formerly Assistant General Counsel at the Central Intelligence Agency and formerly Minority staff director for the House Permanent Select Committee on Intelligence (HPSCI); Robert F. Turner, a former official in the Departments of Defense and State, now professor at the University of Virginia School of Law, where he serves as Associate Director of the Center for National Security Law; and Morton Halperin, fomerly an official in Departments of Defense and State and the National Security Council with service in the Johnson, Nixon and Clinton Administrations, now the Director of U.S. Advocacy for Open Society Institute and a Fellow at the Center for American Progress. On September 18, 2007, testimony was received from Michael McConnell, Director of National Intelligence, and Kenneth L. Wainstein, Assistant Attorney General, National Security Division, Department of Justice.

COMMITTEE CONSIDERATION

On October 10, 2007, the Committee met in open session and ordered the bill H.R. 3773 favorably reported with an amendment, by a roll call vote of 20 to 14, a quorum being present.

COMMITTEE VOTES

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the Committee advises that the following roll call votes occurred during the Committee's consideration of H.R. 3773:

1. An amendment by Mr. Nadler to require the judge who approved the application for foreign intelligence surveillance to assess compliance with the procedures set forth in the certification in support of the application. Adopted 23 to 14.

ROLLCALL NO. 1

	Ayes	Nays	Present
Mr. Conyers, Jr., Chairman	X		
Mr. Berman	X		
Mr. Boucher	X		
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		
Ms. Lofgren	X		
Ms. Jackson Lee	X		
Ms. Waters	X		
Mr. Delahunt	X		
Mr. Wexler	X		
Ms. Sánchez	X		
Mr. Cohen	X		
Mr. Johnson	X		
Ms. Sutton	X		
Mr. Gutierrez	X		
Mr. Sherman	X		
Ms. Baldwin	X		

ROLLCALL NO. 1—Continued

	Ayes	Nays	Present
Mr. Weiner	X		
Mr. Schiff	X		
Mr. Davis	X		
Ms. Wasserman Schultz	X		
Mr. Ellison	X		
Mr. Smith (Texas)		X	
Mr. Sensenbrenner, Jr.		X	
Mr. Coble		X	
Mr. Gallegly			
Mr. Goodlatte		X	
Mr. Chabot			
Mr. Lungren		X	
Mr. Cannon		X	
Mr. Keller		X	
Mr. Issa			
Mr. Pence		X	
Mr. Forbes		X	
Mr. King		X	
Mr. Feeney		X	
Mr. Franks		X	
Mr. Gohmert		X	
Mr. Jordan		X	
Total	23	14	

2. An amendment in the nature of a substitute by Mr. Forbes to establish an alternate statutory scheme to govern the foreign intelligence surveillance activities under FISA, including a provision granting immunity to telecommunications companies for activities subsequent to September 11, 2001 that were conducted pursuant to authorizations from federal intelligence agencies. Defeated 14 to 21.

ROLLCALL NO. 2

	Ayes	Nays	Present
Mr. Conyers, Jr., Chairman		X	
Mr. Berman		X	
Mr. Boucher		X	
Mr. Nadler		X	
Mr. Scott		X	
Mr. Watt		X	
Ms. Lofgren		X	
Ms. Jackson Lee		X	
Ms. Waters		X	
Mr. Delahunt		X	
Mr. Wexler		X	
Ms. Sánchez		X	
Mr. Cohen		X	
Mr. Johnson			
Ms. Sutton		X	
Mr. Gutierrez			
Mr. Sherman		X	
Ms. Baldwin		X	
Mr. Weiner		X	
Mr. Schiff		X	
Mr. Davis		X	
Ms. Wasserman Schultz		X	
Mr. Ellison		X	
Mr. Smith (Texas)	X		
Mr. Sensenbrenner, Jr.	X		
Mr. Coble	X		

ROLLCALL NO. 2—Continued

	Ayes	Nays	Present
Mr. Gallegly			
Mr. Goodlatte	X		
Mr. Chabot			
Mr. Lungren	X		
Mr. Cannon	X		
Mr. Keller	X		
Mr. Issa			
Mr. Pence	X		
Mr. Forbes	X		
Mr. King	X		
Mr. Feeney	X		
Mr. Franks	X		
Mr. Gohmert	X		
Mr. Jordan	X		
Total	14	21	

3. An amendment by Mr. Scott to require the Director of National Intelligence and the Attorney General to submit to the appropriate committees of Congress a description of the primary purpose of the acquisitions for which the application to obtain an order under Section 105B was submitted. Adopted 21 to 12.

ROLLCALL NO. 3

	Ayes	Nays	Present
Mr. Conyers, Jr., Chairman	X		
Mr. Berman	X		
Mr. Boucher			
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		
Ms. Lofgren	X		
Ms. Jackson Lee	X		
Ms. Waters	X		
Mr. Delahunt	X		
Mr. Wexler	X		
Ms. Sánchez	X		
Mr. Cohen	X		
Mr. Johnson	X		
Ms. Sutton	X		
Mr. Gutierrez			
Mr. Sherman			
Ms. Baldwin	X		
Mr. Weiner	X		
Mr. Schiff	X		
Mr. Davis	X		
Ms. Wasserman Schultz	X		
Mr. Ellison	X		
Mr. Smith (Texas)		X	
Mr. Sensenbrenner, Jr.			
Mr. Coble			
Mr. Gallegly			
Mr. Goodlatte		X	
Mr. Chabot		X	
Mr. Lungren	X		
Mr. Cannon		X	
Mr. Keller		X	
Mr. Issa			
Mr. Pence		X	
Mr. Forbes		X	
Mr. King		X	

ROLLCALL NO. 3—Continued

	Ayes	Nays	Present
Mr. Feeney		X	
Mr. Franks		X	
Mr. Gohmert		X	
Mr. Jordan		X	
Total	21	12	

4. An amendment by Mr. Gohmert to strike sections 3 and 4 of the bill, relating to procedures for authorizing acquisitions and emergency acquisitions of communications of non-United States persons located outside the United States. Defeated 16 to 19.

ROLLCALL NO. 4

	Ayes	Nays	Present
Mr. Conyers, Jr., Chairman		X	
Mr. Berman		X	
Mr. Boucher		X	
Mr. Nadler		X	
Mr. Scott		X	
Mr. Watt		X	
Ms. Lofgren		X	
Ms. Jackson Lee		X	
Ms. Waters			
Mr. Delahunt		X	
Mr. Wexler		X	
Ms. Sánchez		X	
Mr. Cohen		X	
Mr. Johnson		X	
Ms. Sutton		X	
Mr. Gutierrez			
Mr. Sherman			
Ms. Baldwin		X	
Mr. Weiner		X	
Mr. Schiff		X	
Mr. Davis			
Ms. Wasserman Schultz		X	
Mr. Ellison		X	
Mr. Smith (Texas)	X		
Mr. Sensenbrenner, Jr.	X		
Mr. Coble	X		
Mr. Gallegly	X		
Mr. Goodlatte	X		
Mr. Chabot	X		
Mr. Lungren			
Mr. Cannon	X		
Mr. Keller	X		
Mr. Issa	X		
Mr. Pence	X		
Mr. Forbes	X		
Mr. King	X		
Mr. Feeney	X		
Mr. Franks	X		
Mr. Gohmert	X		
Mr. Jordan	X		
Total	16	19	

5. On reporting the bill favorably. Agreed to 20 to 14.

ROLLCALL NO. 5

	Ayes	Nays	Present
Mr. Conyers, Jr., Chairman	X		
Mr. Berman	X		
Mr. Boucher	X		
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		
Ms. Lofgren	X		
Ms. Jackson Lee	X		
Ms. Waters			
Mr. Delahunt	X		
Mr. Wexler	X		
Ms. Sánchez	X		
Mr. Cohen	X		
Mr. Johnson	X		
Ms. Sutton	X		
Mr. Gutierrez			
Mr. Sherman			
Ms. Baldwin	X		
Mr. Weiner	X		
Mr. Schiff	X		
Mr. Davis	X		
Ms. Wasserman Schultz	X		
Mr. Ellison	X		
Mr. Smith (Texas)		X	
Mr. Sensenbrenner, Jr.		X	
Mr. Coble		X	
Mr. Gallegly			
Mr. Goodlatte		X	
Mr. Chabot		X	
Mr. Lungren			
Mr. Cannon		X	
Mr. Keller		X	
Mr. Issa			
Mr. Pence		X	
Mr. Forbes		X	
Mr. King		X	
Mr. Feeney		X	
Mr. Franks		X	
Mr. Gohmert		X	
Mr. Jordan		X	
Total	20	14	

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

NEW BUDGET AUTHORITY AND TAX EXPENDITURES

Pursuant to section 4(b)(7), there is authorized to be appropriated $5 million for each of fiscal years 2008 and 2009.

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill, H.R. 3773, the following estimate and comparison prepared

by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, October 12, 2007.

Hon. JOHN CONYERS, Jr.,
Chairman, Committee on the Judiciary,
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,

ROBERT A. SUNSHINE,
(For Peter R. Orszag, Director).

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 requires 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 sur-

veillance, 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 7 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 8 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.
- Section 9 would authorize the appropriation of the amounts necessary to provide personnel and information technology for DOJ and the National Security Agency to submit timely 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 Permanent Select Committee on Intelligence (HPSCI) on October 10, 2007. The language of the two versions of the bill is similar, though this version of the bill does not contain some provisions included in the version approved by the HPSCI.

The version of the bill approved by the HPSCI 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, the version approved by the HPSCI contains authorizations for additional personnel for the Office of the Director of National Intelligence and the Foreign Intelligence Surveillance Court. Both of those provisions could make the cost of the version of H.R. 3773 approved by the HPSCI larger than the cost of the version of the bill approved by the Judiciary Committee.

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.

PERFORMANCE GOALS AND OBJECTIVES

The Committee states that pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 3773 will strengthen the Nation's ability to collect foreign intelligence information and prevent terrorism consistent with the Fourth Amendment to the Constitution and the Nation's commitment to individual liberty.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds the authority for this legislation in article I, section 8, clauses 1, 3, and 9 of the Constitution, as well as the Fourth Amendment.

ADVISORY ON EARMARKS

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.

SECTION-BY-SECTION ANALYSIS

Section 1. Short Title and Table of Contents. Section 1 of the bill sets forth the short title as the Responsible Electronic Surveillance That is Overseen, Reviewed, and Effective Act of 2007 or RESTORE Act of 2007.

Section 2. Clarification of Electronic Surveillance of Non-United States Persons Outside the United States. Section 2 of the bill amends section 105A of FISA to address two situations: (1) "foreign-to-foreign" communications, and (2) foreign communications that involve or potentially involve U.S. communications ("one-end-foreign" or "one-end-potentially-U.S."). This section replaces section 105A of FISA, as amended by the PAA. And by making these clarifications stand alone, rather than amending the definition of electronic surveillance as did the PAA, this section avoids the collateral effect on other parts of FISA, such as Section 106 (governing the use and dissemination of U.S. person communications).

Revised section 105A(a) clarifies that a court order is not required for the acquisition of the contents of communications between two non-U.S. persons located outside the United States, even where the surveillance device itself is located in the United States.

Revised section 105A(b) provides that electronic surveillance of non-U.S. persons reasonably believed to be outside the United States, conducted for the purpose of collecting foreign intelligence information, must be done in accordance with court orders approved pursuant to section 105B or, in an emergency, section 105C. This provision limits the definition of "foreign intelligence information" to those forms described in section 101(e)(1) and (2)(A) of FISA [national security concerns such as terrorism, espionage or defense], to protect communications that merely concern foreign affairs, such as trade negotiations, business deals, or political visits.

Section 3. Procedures for Authorizing Acquisitions of Communications of Non-United States Persons Located Outside the United States. Section 3 of the bill amends 105B of FISA to set forth procedures for authorizing acquisitions. The authorization must be issued by the FISA Court, as opposed to the Director of National Intelligence (DNI) or the Attorney General (AG) as currently provided in the PAA. Application requirements, standards of review, and scope of the authorization are specified in this section, which defines the roles of the Government, the court, and the telecommunications providers.

Revised section 105B(a) provides that the DNI and the AG may apply for a court order to authorize the collection of communications of persons reasonably believed to be located outside the United States, conducted for the purpose of collecting foreign intelligence information as provided in Section 101(e)(1) and (2)(A) of FISA.

Revised section 105B(b) specifies the requirements for the contents of an application under section 105B(a) with respect to the scope of the authorized acquisitions, the minimization and dissemination safeguards, and the requirement to obtain a FISA warrant when targeting U.S. persons' communications.

First, the application must contain a certification from the DNI and the AG that: (1) the targets of acquisition are reasonably believed to be outside the United States; (2) the targets of acquisition

are not known United States persons; (3) the acquisition involves obtaining the assistance of communications service providers; and (4) that a significant purpose of the acquisition is to obtain foreign intelligence information as provided in Section 101(e)(1) and (2)(A) of FISA. Targets of this surveillance include radical jihadist groups, nuclear proliferators, hostile foreign governments, and narco-terrorists.

Second, the application must contain a description of: (1) the procedures that will be used to determine that there is a reasonable belief that the target of the acquisition is located outside the United States; (2) the nature of the information sought, including the foreign power against which acquisition will be directed; (3) minimization procedures that will be used, consistent with section 101(h) of FISA; and (4) the guidelines that will be used to ensure that a FISA warrant will be sought when a significant purpose of the acquisition is to acquire the communications of a specific person reasonably believed to be located in the United States. Revised section 105B(c) provides that, as in the PAA, these declarations need not include specific facilities, places, or premises where the acquisition will be directed.

Revised 105B(d) requires that the FISA Court review an application within 15 days, and approve it if the following criteria are met: (1) the procedures to determine whether the targets of acquisition are located outside the United States are reasonably designed to meet that goal; (2) the proposed minimization procedures satisfy the definition of minimization procedures in section 101(h) of FISA, and (3) the guidelines to ensure that a FISA warrant will be sought when a significant purpose of the acquisition is to acquire the communications of a specific person reasonably believed to be located in the United States are also reasonably designed to meet that goal.

Revised section 105B(e) provides that the resulting order must: (1) authorize the acquisition as requested or as modified by the judge; (2) require the assistance of a communications service provider who has authorized access to the information or facilities sought; (3) require the service provider to maintain security over any records concerning the acquisition; (4) direct the government to compensate the service provider and to provide them with a copy of the court order, and (5) direct the government to follow the procedures and guidelines that it relied on in its application, as approved or modified by the court.

Revised section 105B(e) also empowers the AG to invoke the aid of the FISA Court to compel a communications service provider to comply with the Court's order. It also provides prospective liability protection by establishing that no cause of action shall lie against any service provider for complying with a court order issued under this section. It also requires the DNI and the FISA Court to retain such orders for at least 10 years, and empowers the Court to assess compliance with the minimization procedures and guidelines that it had approved, by reviewing the circumstances under which U.S. person communications were handled under the authorization.

Section 4. Emergency Authorization of Acquisitions of Communications of Non-United States Persons Located Outside the United States. Section 4 of the bill amends section 105C of FISA.

Revised Section 105C(a) allows for an emergency authorization of overseas collection by the DNI and AG, but requires that they submit an application consistent with section 105B within 7 days after authorizing the emergency acquisition.

Revised section 105C(b) empowers the DNI and the AG to authorize emergency acquisition of foreign intelligence information for a period of no more than 45 days if they determine: that an emergency situation exists in respect to a section 105B collection; that the targets of the acquisition are reasonably believed to be outside the United States; that there are reasonable procedures in place to determine that the targets of the acquisition are reasonably believed to be outside the United States; that targets of the acquisition are not known to be United States persons; that the acquisition involves obtaining the assistance of communications service providers; that a significant purpose of the acquisition is to obtain foreign intelligence information under section 101(e)(1) and (2)(A); that minimization procedures to be used meet the definition of minimization procedures under section 101(h) of FISA; and that there are guidelines that will be used to ensure that an application under Section 104 of FISA is filed when the government seeks to conduct electronic surveillance of a person reasonably believed to be located in the United States. Section 105C(b) also requires that, in addition to the requirement to submit a formal 105B application within 7 days, the DNI and the AG must inform the FISA Court of the emergency authorization at the time it is issued.

Revised section 105C(c) provides that the AG may direct a communications service provider to render assistance in conducting the emergency acquisition, and maintain security over any records concerning the emergency acquisition.

Section 5. Oversight of Acquisitions of Communications of Non-United States Persons Located Outside of the United States. Section 5 of the bill adds a new section 105D to FISA.

New section 105D(a) requires that, within 7 days of submitting a section 105B application to the FISA Court, the DNI and the AG must submit to the appropriate committees of Congress a copy of the application (including the certification under section 105B(b)) and a copy of the order issued, including the procedures and guidelines referred to in 105B(d).

New section 105D(b) requires the Inspector General of the Justice Department to conduct quarterly audits of the implementation of and compliance with the guidelines referred to in section 105B(d), and mandates that the results of such audits shall be reported to the appropriate committees of Congress, the DNI, the AG, and the FISA Court. This audit must include: (1) a list of any targets of acquisition that were determined to be located in the United States; (2) the number of persons located in the United States whose communications were intercepted under section 105B; (3) the number of reports disseminated that contained information on United States persons that was collected under section 105B, and (4) the number of applications submitted for approval of electronic surveillance under section 104 of FISA that were based upon information collected under section 105B authorizations. The AG is tasked with providing a report of such audit no later than 30 days after the completion of an audit, to the appropriate committees of Congress.

New section 105D(c) requires the DNI and the AG to submit to the appropriate committees of Congress and the FISA Court 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 section 105B(d) or by a person directed to provide information, facilities, or technical assistance pursuant to an order issued under section 105B or an authorization under section 105C. This report must be submitted no later than 60 days after enactment and every 120 days thereafter.

New section 105D(d) defines "appropriate committees of Congress" to mean the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, the House Judiciary Committee, and the Senate Judiciary Committee.

Section 6. Foreign Intelligence Surveillance Court En Banc. Section 6 of the bill amends section 103C of FISA to authorize the FISA Court, in its discretion, to sit *en banc* to review applications and issue orders.

Section 7. Audit of Warrantless Surveillance Programs. Section 7 of the bill requires the Inspector General of the Justice Department to conduct an audit of all electronic surveillance programs conducted without a warrant since September 11, 2001, including the Terrorist Surveillance Program, within 180 days of enactment. As a part of this audit, the Inspector General shall acquire all documents relevant to these programs. Within 30 days of completing the audit, the IG is to submit an audit report, and the documents, to the appropriate committees of Congress. To facilitate this audit, the DNI is tasked with ensuring that the process for granting necessary clearances for the Inspector General and appropriate staff is conducted as expeditiously as possible.

Section 8. Record-keeping for Acquisition of Communications of United States Persons. Section 8 of the bill requires the DNI and the AG to develop and maintain a system to keep records of the instances where the identity of U.S. persons whose communications were intercepted without a warrant have been disclosed to other government departments or agencies, and requires an annual report to Congress on this record-keeping effort.

Section 9. Authorization for Increased Resources Relating to Foreign Intelligence Surveillance Act. Section 9 of the bill authorizes appropriations for the Justice Department and the National Security Agency to meet resource demands associated with submitting applications to the FISA Court and fulfilling the bill's audit and reporting requirements.

Section 10. Reiteration of FISA as the Exclusive Means by which Electronic Surveillance May be Conducted for Gathering Foreign Intelligence Information. Section 10 of the bill reiterates that FISA is the exclusive means for conducting electronic surveillance for purposes of collecting foreign intelligence information, and specifies that explicit statutory authorization is required in order to establish an exception to FISA.

Section 11. Technical and Conforming Amendments. Section 11 of the bill amends the table of contents in FISA to include titles for sections 105A–D; revises a reference to the FISA Court added by the PAA, to provide jurisdiction to review applications submitted under section 105B; and repeals the reporting requirements and transition procedures established under the PAA.

Section 12. Sunset; Transition Procedures. Section 12 provides that these revisions sunset on December 31, 2009, with the exception that any section 105B authorizations in effect on that date are valid through the date of expiration of the particular order. Section 12 also provides that any authorization issued under section 105B that was in effect prior to the enactment of the bill (that is, issued under the PAA) shall remain in effect until the authorization's expiration or until 180 days after the date of enactment of the RESTORE Act, whichever is earlier.

CHANGES IN EXISTING LAW 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, H.R. 3773, 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 changes are 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

* * * * * * *

DESIGNATION OF JUDGES

SEC. 103. (a) * * *

* * * * * * *

(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 Intelligence 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 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 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 judge shall 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 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) a copy of the application, including the certification made under section 105B(b)(1); and

(B) a description of the primary purpose of the acquisition for which the application is submitted; 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 12(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).]

* * * * * * *

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)).]

DISSENTING VIEWS

In August, Congress passed the "Protect America Act of 2007," which filled a gap in existing law. The bill: (1) affirmed well-established law that neither the Constitution nor federal law requires a court order to gather foreign communications from foreign terrorists; (2) adopted flexible procedures to collect foreign intelligence from foreign terrorists overseas; and (3) provided for court review of collection procedures under this new authority. The Director of National Intelligence Admiral Mike McConnell made it clear that these reforms were essential for the Intelligence Community to protect America from terrorist attack.[1] The majority in large part acceded to Admiral McConnell's request but tacked on a 180-day sunset provision.

Admiral McConnell has explained to Congress for more than a year that due to recent FISA court decisions, the government must now devote substantial resources to obtaining court approvals—based on a showing of probable cause—to conduct surveillance against terrorists located overseas in some circumstances. This is contrary to what Congress intended when it enacted FISA and has come about simply because of a change in technology. The government does not know in advance whom these terrorists will talk to and needs to have the flexibility to monitor calls that may occur between a foreign terrorist and a terrorist inside the United States. Such monitoring of these communications can be conducted with well-established minimization rules that have been applied to restrict any unwarranted intrusion on the civil liberties of any United States citizens. Requiring specific applications and authority for surveillance of such communications would impose burdens and delays with possible catastrophic consequences.

Some groups and newspaper editors have, in the name of protecting civil liberties, spent the last month spreading false allegations and misconceptions about foreign surveillance to foster opposition to the Protect America Act. Such claims are irresponsible.

We are a nation at war with foreign terrorists who continue to plan deadly attacks against America. The safety of Americans depends on action by Congress. Foreign terrorists are committed to the destruction of our country. To defeat them, our Intelligence Community must have the necessary tools to detect and disrupt such attacks.

We have a responsibility in Congress to prevent attacks against our country and protect our communities and our families. Civil liberties are the foundation of our freedom, but such freedom will

[1] Admiral McConnell's intelligence and national security career spans over 30 years. He has served under both Democratic and Republican Presidents, including as the Director of the National Security Agency in the Clinton Administration. Despite his impressive, non-partisan service in the Intelligence Community, Democrats have impugned his motives and his integrity purely for partisan gain. Such criticisms are unfair and distract from what should be a non-partisan issue—protecting our country from terrorist attacks.

never exist if we have no security. We all cherish our individual liberties. But our liberties cannot flourish without security. The pursuit of life, liberty and happiness can only occur with peace of mind and a safe and secure country.

This fall we had two full Judiciary Committee hearings on the Protect America Act. Admiral McConnell testified that prior to the Act, the Intelligence Community was not collecting approximately two-thirds of the foreign intelligence information that it used to collect before recent legal interpretations required the government to obtain FISA court orders for overseas surveillance. In addition, Admiral McConnell urged Congress to enact the Administration's FISA modernization legislation submitted in April.

The RESTORE Act of 2007 ignores the Administration's April submission and Admiral McConnell's testimony at the oversight hearing. It would significantly limit the Intelligence Community from conducting foreign intelligence collection, improperly inject the FISA court into review of operational details and expand oversight responsibilities to unqualified entities.

It is striking how the majority has acted when it comes to protecting our country from terrorists, spies and other enemies. These are not issues that should be sacrificed to talking points, politics and the satisfaction of liberal lobbying interests. We should be passing effective bipartisan legislation, supported by Admiral McConnell, to protect our national security.

Telecommunications technology has evolved rapidly in the last 30 years. Terrorist tactics are constantly changing in response to our efforts to disrupt their plots. Essential tools that we use must be modernized to keep up with the changing environment.

The American people understand what is at stake—nearly 60 percent of Americans polled on the subject of FISA reform supported the Protect America Act. Less than 35 percent opposed it. The simple fact is that Americans support surveillance of foreign terrorists when they contact persons in the United States.

The RESTORE Act in fact restores nothing. The safety of Americans depends on responsible action by Congress. The majority has ignored the need for modernizing the Foreign Intelligence Surveillance Act. Rather, it has adopted rhetoric that boils down to political cover at the expense of national security.

The RESTORE Act is flawed in so many respects that we will address only the most significant problems with the bill.

First, the RESTORE Act requires the Intelligence Community to obtain FISA court orders for foreign communications of persons reasonably believed to be outside the United States. Since it was enacted in 1978, FISA never required the government to acquire court orders for such communications, and the legislative history and subsequent Court decisions support that view. It is irresponsible to extend constitutional protections under the 4th Amendment to terrorists, spies and other enemies overseas—an unprecedented act that will threaten our country's security.

At the oversight hearing, Admiral McConnell stated that such a solution is unworkable and impractical. He explained that this was not because of a "resource" limitation but was because of the need to collect and analyze foreign intelligence information on a timely basis so that threats can be identified and acted upon.

FISA does not require a court order to gather foreign communications between foreign terrorists outside the United States. The majority repeats this undisputed fact to deflect discussion of the real issue—should FISA require a court order when a foreign terrorist communicates with an unknown person at an unknown location? The RESTORE Act says yes. The Intelligence Community and 30 years of experience under FISA say no. For the last 30 years FISA never required such an order, and the majority's push now to require a court order threatens our nation's safety.

The majority shows no concern for the impact such a requirement will have on the Intelligence Community. Requiring a court order for every phone call from a foreign target to a person inside the U.S. is contrary to FISA as it has operated for 30 years and contrary to common sense—how can the Intelligence Community anticipate a communication from a foreign terrorist to a terrorist inside our country?

In much the same way as a criminal wiretap, FISA provides—and has provided for 30 years—specific minimization procedures to protect the privacy of persons inside the United States with whom a foreign target may communicate. It is unclear why now, after all this time, the majority now seeks to dismantle rather than modernize FISA.

Requiring separate FISA authority for these calls would be a deadly mistake. Calls between a foreign terrorist and a person located inside the United States should be minimized in accordance with well established procedures. To do otherwise is to jeopardize the safety of our nation.

Second, the RESTORE Act omits any retrospective liability protection for telephone companies and other carriers that assisted the government after September 11, 2001. These companies deserve our thanks, not a flurry of lawsuits seeking access to documents the disclosure of which would harm our country. The majority promised Admiral McConnell that this issue would be addressed in this legislation, and the majority has reneged on its promise.

Third, the RESTORE Act injects the FISA Court into reviewing and approving the Intelligence Community's procedures for (1) minimization; and (2) "guidelines" for determining that there is a reasonable basis to believe that the telephone is located outside the United States. This is unprecedented and will only burden the Intelligence Community with court review of operational details that will only delay FISA court approval of surveillance orders, all to the detriment of our security.

Fourth, the RESTORE Act authorizes the FISA court to conduct wholesale reviews of how the Intelligence Community "acquires, retains and disseminates" foreign intelligence information. The FISA court plays a critical role in providing judicial review of the government's FISA applications in specific cases. But this proposed expansion gives the Court a "super-supervision" role that is inappropriate and unnecessary.

Fifth, the RESTORE Act inexplicably creates a new sunset—December 31, 2009. This is a mistake. If Congress needs to change the law, then it should do so, notwithstanding any sunset. Terrorists do not lay down their arms or change their objectives when a

sunset fast approaches, and neither should the United States abandon tools on a date certain in the future.

Sixth, the RESTORE Act requires the Justice Department's Inspector General to conduct (1) quarterly audits of the Intelligence Community's compliance with the requirements of the new Act; and (2) an audit of all surveillance activities conducted without a warrant after September 11, 2001. We respect the DOJ IG's work on a number of issues. However, the DOJ IG does not have the expertise or knowledge of the FISA process, the Intelligence Community's activities, and inner-workings of various agencies to be able to conduct meaningful reviews. Moreover, the intelligence agencies (e.g. CIA, NSA) already have Inspector Generals who conduct regular audits and will continue to do so even if this provision was enacted.

Seventh, the RESTORE Act requires the DNI and the Justice Department to submit reports every 120 days on foreign surveillance operations, including any instance of non-compliance with any court requirement. The DNI and Justice Department are already required to provide detailed information on such surveillance to the Senate and House Intelligence Committees, and there is no need to increase that requirement.

Lastly, the RESTORE Act requires the Justice Department and the Intelligence Community to create a new database that records every instance in which the identity of a United States person whose communications was collected is disclosed to other agencies and for what purpose. This proposal is misguided—while attempting to protect American's civil liberties, it may have the opposite effect by establishing a single database that lists all Americans who have been identified in foreign intelligence information and whose identity has been disclosed to other agencies.

Such disclosures may not reflect that the person has been identified as a suspected terrorist or a spy; it may be that the person's identity is a lead needed to collect important information concerning another person's activities. The majority does not explain why such a database is needed, why such records are important, and how such records will be protected from unauthorized or inadvertent disclosures.

We can only hope that the majority will take the RESTORE Act and go back to the drawing board. As currently drafted, the majority's proposal is irresponsible, ignores well-established practices governing the collection of foreign intelligence information, and in the end will embolden and enhance our enemies' ability to carry out deadly plots without fear of being detected.

We should maintain our commitment to winning the war against terrorism. George Washington once said, "There is nothing so likely to produce peace as to be well prepared to meet the enemy." Heeding his words, we must maintain our commitment to winning the war against terrorism.

FISA MODERNIZATION

Last April, Admiral McConnell submitted to Congress a comprehensive proposal to modernize FISA. That proposal should have been enacted.

When Congress drafted FISA in 1978, it framed critical definitions (most importantly, the definition of "electronic surveillance") in terms of the specific communications technology in use at the time. As a result, the application of FISA depends heavily on the technology used to communicate. Sweeping changes in telecommunications technology have occurred since 1978. These changes were not and could not have been anticipated by Congress.

The Administration's proposed bill would amend the definition of "electronic surveillance" in a manner that restores FISA's original focus on the domestic communications of persons within the United States. Importantly, the amended definition would not depend on the technologies now in use and would continue to maintain the right focus as technology changes.

The bill also streamlines the FISA application process. It would eliminate the unnecessary burden that the current statute places on the government. Applications should contain only the information the FISA Court needs to make its determinations.

The bill would provide liability protection to communications providers that are alleged to have assisted the government with authorized intelligence activities since 9/11. Those companies deserve our appreciation—not a deluge of lawsuits.

In addition, the bill would amend the definition of "agent of a foreign power" to allow surveillance of non-US persons who possess significant foreign intelligence information. The bill also would modify the definition to include persons who engage in the proliferation of weapons of mass destruction.

Finally, the bill would provide for the transfer of cases involving the legality of classified communications intelligence activities from regular courts to the FISA Court. This will help protect classified information and allow cases to proceed before the court most familiar with communications intelligence activities and most practiced in safeguarding the type of national security information involved.

AMENDMENTS

Republican Members offered two amendments at markup. The first, offered by Mr. Forbes of Virginia, was an amendment in the nature of a substitute that incorporated the Administration's FISA modernization proposal. The second, offered by Mr. Gohmert of Texas, struck sections 3 and 4 of the underlying bill. Both amendments were defeated by recorded vote. Below is a summary of the substitute amendment.

Section 1. Short Title. This section cites the title of the Act as the "Foreign Intelligence Surveillance Modernization Act of 2007."

Section 2. Definitions. This section amends the definition of "agent of a foreign power" to include non-United States persons who possess or receive significant foreign intelligence information while in the United States. This amendment would ensure that the United States government can collect necessary information possessed by a non-United States person visiting the United States.

This section also redefines the term "electronic surveillance" in a technology-neutral manner to refocus FISA on the communications of individuals in the United States. When FISA was enacted in 1978, Congress used language that was technology-dependent and related specifically to the telecommunications systems that ex-

isted at that time. As a result of revolutions in communications technology since 1978, and not any considered judgment of Congress, the current definition of "electronic surveillance" sweeps in surveillance activities that Congress actually intended to *exclude* from FISA's scope.

Section 2 provides a new, technology-neutral definition of "electronic surveillance" focused on the core question of *who* is the subject of the surveillance, rather than on *how* or *where* the communication is intercepted. Under the amended definition, "electronic surveillance" would encompass:

> (1) the installation or use of an electronic, mechanical, or other surveillance device for acquiring information by intentionally directing surveillance at a particular, known person who is reasonably believed to be located within the United States under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; or
>
> (2) the intentional acquisition of the contents of any communication under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, if both the sender and all intended recipients are reasonably believed to be located within the United States.

Finally, section 2 also amends the definition of the terms "minimization procedures" and "content" to conform to other changes in this proposal or provisions in Title 18.

Section 3. Attorney General Authorization for Electronic Surveillance. This section alters the circumstances in which the Attorney General can exercise his authority—present in FISA since its passage—to authorize electronic surveillance without a court order. Currently, subsection 102(a) of FISA allows the Attorney General to authorize electronic surveillance without a court order where the surveillance is "solely directed" at the acquisition of the contents of communications "transmitted by means of communications used *exclusively*" between or among certain types of traditional foreign powers.

As a consequence, the government must generally seek FISA Court approval for the same sort of surveillance today. It is important to note that the proposed amendment to this provision of FISA would not alter the types of "foreign powers" to which this authority applies. It still would apply only to foreign governments, factions of foreign nations (not substantially composed of United States persons), and entities openly acknowledged by a foreign government to be directed and controlled by a foreign government or governments.

This section also creates new procedures (those proposed in new sections 102A and 102B) pursuant to which the Attorney General could authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States, under circumstances in which the acquisition does not constitute "electronic surveillance" under FISA.

This critical change works hand in glove with the new definition of "electronic surveillance" in section 2. FISA currently provides a

mechanism for the government to obtain a court order compelling communications companies to assist in conducting electronic surveillance. Because the proposed legislation would reduce the scope of the definition of "electronic surveillance," certain activities that previously were "electronic surveillance" under FISA would fall out of the statute's scope. This new provision would provide a mechanism for the government to obtain the aid of a court to ensure private sector cooperation with these lawful intelligence activities no longer covered by the definition of "electronic surveillance." The new section would also provide a means for third parties receiving such a directive to challenge the legality of that directive in court.

Section 4. Jurisdiction of FISA Court. This section makes two relatively minor amendments to FISA. First, it amends section 103(a) of FISA to provide that judges on the FISA Court shall be drawn from "at least seven" of the United States judicial circuits. The current requirement—that judges be drawn from seven different judicial circuits—unnecessarily complicates the designation of judges for that important court.

This section also moves to section 103 of FISA, with minor amendments, a provision that currently appears in section 102. New section 103(g) would provide that applications for a court order under section 104 of FISA are authorized if the Attorney General approves the applications to the FISA Court, and a judge to whom the application is made may grant an order approving electronic surveillance in accordance with the statute—a provision that is most suitably placed in section 103 of FISA, which pertains to the FISA Court's jurisdiction.

The new provision would eliminate the restriction on the FISA Court's jurisdiction in 50 U.S.C. § 1802(b), which provides that the court cannot grant an order approving electronic surveillance directed at the types of foreign powers described in section 102(a) unless the surveillance may involve the acquisition of communications of a United States person. Although the government still would not be required to obtain FISA Court orders for surveillance involving those types of foreign powers, the removal of this restriction would permit the government to seek FISA Court orders in those circumstances when an order is desirable.

Section 5. Application for Court Orders. The current procedure for applying to the FISA Court for a surveillance order under section 104 of FISA should be streamlined. While FISA should require the government to provide information necessary to establish probable cause and other essential FISA requirements, FISA requires the government to provide information that is not necessary to these objectives. Section 5 attempts to increase the efficiency of the FISA application process in several ways.

First, the government currently is required to provide significant amounts of information that serves little or no purpose in safeguarding civil liberties. By amending FISA to require only summary descriptions or statements of certain information, the burden imposed on applicants for a FISA Court order authorizing surveillance will be substantially reduced. For example, section 5 amends the current FISA provision requiring that the application contain a "detailed description of the nature of the information sought,"

and would allow the government to submit a summary description of such information.

Section 5 similarly would amend the current requirement that the application contain a "statement of facts concerning all previous applications" involving the target, and instead would permit the government to provide a summary of those facts. While these amendments would help streamline FISA by reducing the burden involved in providing the FISA Court with information that is not necessary to protect the privacy of U.S. persons in the United States, the FISA Court would still receive the information it needs in considering whether to authorize the surveillance.

Section 5 also increases the number of individuals who can make FISA certifications. Currently, FISA requires that such certifications be made only by senior Executive Branch national security officials who have been confirmed by the Senate. The new provision would allow certifications to be made by individuals specifically designated by the President and would remove the restriction that such individuals be Senate-confirmed. As this committee is aware, many intelligence agencies have an exceedingly small number of Senate confirmed officials (sometimes only one, or even none), and the Administration's proposal would allow intelligence agencies to more expeditiously obtain certifications.

Section 6. Issuance of an Order. This section amends the procedures for the issuance of an order under section 105 of FISA to conform with the changes to the application requirements that would be effected by changes to section 104 discussed above.

This section also extends the initial term of authorization for electronic surveillance of a non-United States person who is an agent of a foreign power from 120 days to one year. This change reduces the time spent preparing applications for renewals relating to non-United States persons, thereby allowing more resources to be devoted to cases involving United States persons.

Section 6 also allows any FISA order to be extended for a period of up to one year. This change reduces the time spent preparing applications to renew FISA orders that already have been granted by the FISA Court, thereby increasing the resources focused on initial FISA applications. Additionally, section 6 makes important amendments to the procedures by which the Executive Branch may initiate emergency authorizations of electronic surveillance prior to obtaining a court order. Currently the Executive Branch has 72 hours to obtain court approval after emergency surveillance is initially authorized by the Attorney General. The amendment extends the emergency period to seven days. This change will help ensure that the Executive Branch has sufficient time in an emergency situation to accurately prepare an application, obtain the required approvals of senior officials, apply for a court order, and satisfy the court that the application should be granted.

This provision also modifies the existing provision that allows certain information to be retained when the FISA Court rejects an application to approve an emergency authorization. Presently, such information can be retained if it indicates a threat of death or serious bodily harm to any person. The proposed amendment would also permit such information to be retained if the information is "significant foreign intelligence information" that, while important

to the security of the country, may not rise to the level of death or serious bodily harm.

Finally, section 6 adds a new paragraph that requires the FISA Court, when granting an application for electronic surveillance, to simultaneously authorize the installation and use of pen registers and trap and trace devices if such is requested by the government. This technical amendment results from the proposed change in the definition of "contents" in Title I of FISA. And, of course, as the standard to obtain a court order for electronic surveillance is substantially higher than the pen-register standard, there should be no objection to an order approving electronic surveillance that also encompasses pen register and trap and trace information.

Section 7. Use of Information. This section amends subsection 106(i) of FISA, which pertains to limitations regarding the use of unintentionally acquired information. Currently, subsection 106(i) provides that lawfully but unintentionally acquired *radio* communications between persons located in the United States must be destroyed unless the Attorney General determines that the communications indicate a threat of death or serious bodily harm. Section 7 amends subsection 106(i) by making it technology-neutral; we believe that the same rule should apply regardless how the communication is transmitted. The amendment also allows for the retention of unintentionally acquired information if it "contains significant foreign intelligence information." This ensures that the government can retain and act upon valuable foreign intelligence information that is collected unintentionally, rather than being required to destroy all such information that does not fall within the current exception.

Section 7 also clarifies that FISA does not preclude the government from seeking protective orders or asserting privileges ordinarily available to protect against the disclosure of classified information. This is necessary to clarify any ambiguity regarding the availability of such protective orders or privileges in litigation.

Section 8. Weapons of Mass Destruction. This section amends sections 101, 106, and 305 of FISA to address concerns related to weapons of mass destruction. These amendments reflect the threat posed by these catastrophic weapons and would extend FISA to apply to individuals and groups engaged in the international proliferation of such weapons. Section 8 amends section 101 of FISA to include a definition of the term "weapon of mass destruction."

Section 8 also amends the section 101 definitions of "foreign power" and "agent of a foreign power" to include groups and individuals (other than U.S. persons) engaged in the international proliferation of weapons of mass destruction. Section 8 similarly amends the definition of "foreign intelligence information." Finally, section 8 would amend sections 106 and 305 of FISA, which pertain to the use of information, to include information regarding the international proliferation of weapons of mass destruction.

Section 9. Liability Defense. This section provides litigation protections to telecommunications companies that are alleged to have assisted the government with classified communications intelligence activities in the wake of the September 11th terrorist attacks. Telecommunications companies have faced numerous law-

suits as a result of their alleged activities in support of the government's efforts to prevent another terrorist attack. If private industry partners are alleged to cooperate with the government to ensure our nation is protected against another attack, they should not be held liable for any assistance they are alleged to have provided.

Section 10. Amendments for Physical Searches. This section amends section 303 of FISA (50 U.S.C. 1823), which relates to physical searches, to streamline the application process, update and augment the emergency authorization provisions, and increase the potential number of officials who can certify FISA applications. These changes largely parallel those proposed to the electronic surveillance application process. For instance, they include amending the procedures for the emergency authorization of physical searches without a court order to allow the executive branch seven days to obtain court approval after the search is initially authorized by the Attorney General.

This section also amends section 304 of FISA, pertaining to orders authorizing physical searches, to conform to the changes intended to streamline the application process. Additionally, section 10 permits the search of not only property that *is* owned, used, possessed by, or in transit to or from a foreign power or agent of a foreign power, but also property that is *about* to be owned, used, possessed by, or in transit to or from these powers or agents. This change makes the scope of FISA's physical search provisions coextensive with FISA's electronic surveillance provisions in this regard.

Section 11. Amendments for Emergency Pen Registers and Trap and Trace Devices. This section amends the procedures found in section 403 of FISA (50 U.S.C. 1843) regarding the emergency use of pen registers and trap and trace devices without court approval to allow the executive branch seven days to obtain court approval after the emergency use is initially authorized by the Attorney General. (The current period is 48 hours.) This change would ensure the same flexibility for these techniques as would be available for electronic surveillance and physical searches.

Section 12. Mandatory Transfer for Review. This section allows for the transfer of sensitive national security litigation to the FISA Court in certain circumstances. This provision requires a court to transfer a case to the FISA Court if: (1) the case is challenging the legality of a classified communications intelligence activity relating to a foreign threat, or the legality of any such activity is at issue in the case, and (2) the Attorney General files an affidavit under oath that the case should be transferred because further proceedings in the originating court would harm the national security of the United States.

By providing for the transfer of such cases to the FISA Court, section 12 ensures that, if needed, judicial review may proceed before the court most familiar with communications intelligence activities and most practiced in safeguarding the type of national security information involved. Section 12 also provides that the decisions of the FISA Court in cases transferred under this provision would be subject to review by the FISA Court of Review and the Supreme Court of the United States.

Section 13. Technical and Conforming Amendments. This section makes technical and conforming amendments to sections 103, 105, 106, and 108 of FISA (50 U.S.C. 1803, 1805, 1806, 1808).

Section 14. Effective Date. This section provides that these amendments shall take effect 90 days after the date of enactment of the Act, and that orders in effect on that date shall remain in effect until the date of expiration. It would allow for a smooth transition after the proposed changes take effect.

Section 15. Construction; Severability. This section provides that any provision of this Act held to be invalid or unenforceable shall be construed so as to give it the maximum effect permitted by law, unless doing so results in a holding of utter invalidity or unenforceability, in which case the provision shall be deemed severable and shall not affect the remaining sections.

SUMMARY

For all of these reasons, we urge our colleagues to reject the RESTORE Act and enact the Administration's proposal. The lives of Americans depend on it.

LAMAR SMITH.
F. JAMES SENSENBRENNER, JR.
HOWARD COBLE.
ELTON GALLEGLY.
STEVE CHABOT.
DANIEL E. LUNGREN.
CHRIS CANNON.
DARRELL ISSA.
J. RANDY FORBES.
TOM FEENEY.
LOUIE GOHMERT.
JIM JORDAN.

○