FISA MODERNIZATION PROVISIONS OF THE PROPOSED FISCAL YEAR 2008 INTELLIGENCE AUTHORIZATION

TITLE IV - MATTERS RELATING TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.

Sec.	400.	Short Title.
Sec.	401.	Definitions.
Sec.	402.	Attorney General Authorization for Electronic Surveillance.
Sec.	403.	Jurisdiction of FISA Court.
Sec.	404.	Applications for Court Orders.
Sec.	405.	Issuance of an Order.
Sec.	406.	Use of Information.
Sec.	407.	Weapons of Mass Destruction.
Sec.	408.	Liability Defense.
Sec.	409.	Amendments for Physical Searches.
Sec,	410.	Amendments for Emergency Pen Registers and Trap and Trace Devices.
Sec.	411.	Mandatory Transfer for Review
Sec.	412.	Technical and Conforming Amendments.
Sec.	413.	Effective Date.
Sec.	414.	Construction; Severability.

SEC. 400. SHORT TITLE

Sections 400 through 414 may be cited as the ''Foreign Intelligence Surveillance Modernization Act of 2007''.

SEC. 401. DEFINITIONS.

- (a) AGENT OF A FOREIGN POWER.—Subsection (b)(1) of section
 101 of the Foreign Intelligence Surveillance Act of 1978
 (50 U.S.C. 1801) is amended—
- (1) in subparagraph (B), by striking ``; or'' and
 inserting ``;''; and
 - (2) by adding at the end the following:
 - ''(D) is reasonably expected to possess, control, transmit, or receive foreign intelligence information while such person is in the United States, provided that the certification required under section 104(a)(6) or 303(a)(6) contains a description of the kind of significant foreign intelligence information sought;''.
- (b) ELECTRONIC SURVEILLANCE.—Subsection (f) of such section is amended to read as follows:
 - ''(f) 'Electronic surveillance' means-
 - "(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.''.
- (c) WIRE COMMUNICATION. -Subsection (1) of such section is amended by striking subsection (1).
- (d) MINIMIZATION PROCEDURES.—Subsection (h) of such section is amended—
- (1) in subsection (3) by striking "; and" and
 inserting "."; and
 - (2) by striking subsection (4).
- (e) CONTENTS.—Subsection (n) of such section is amended to read as follows:
 - ''(n) 'Contents', when used with respect to a communication, includes any information concerning the substance, purport, or meaning of that communication.''

SEC. 402. ATTORNEY GENERAL AUTHORIZATION FOR ELECTRONIC SURVEILLANCE.

- (a) IN GENERAL.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is further amended by striking section 102 and inserting the following:
 - ''AUTHORIZATION FOR ELECTRONIC SURVEILLANCE FOR
 FOREIGN INTELLIGENCE PURPOSES
 - ''SEC. 102. (a) IN GENERAL.— Notwithstanding any other law, the President, acting through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for periods of up to one year if the Attorney General—
 - '`(1) certifies in writing under oath that'`(A) the electronic surveillance is
 directed at-
 - ''(i) the acquisition of the contents
 of communications of a foreign power,
 as defined in paragraph (1), (2), or
 (3) of section 101(a); or
 ''(ii) the acquisition of technical
 intelligence, other than the spoken
 communications of individuals, from
 property or premises under the control

of a foreign power, as defined in paragraph (1), (2), or (3) of section 101(a); and

- ''(B) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 101(h); and
- "(2) reports such minimization procedures and any changes thereto to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate at least 30 days prior to the effective date of such minimization procedures, unless the Attorney General determines immediate action is required and promptly notifies the committees of such minimization procedures and the reason for their becoming effective immediately.
- ''(b) MINIMIZATION PROCEDURES.—An electronic surveillance authorized under this section may be conducted only in accordance with the Attorney General's certification and the minimization procedures. 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 the provisions of section 108(a).

- "(c) SUBMISSION OF CERTIFICATION.—The Attorney General shall promptly transmit under seal to the court established under section 103(a) a copy of the certification under subsection (a)(1). Such certification shall be maintained under security measures established by the Chief Justice with the concurrence of the Attorney General, in consultation with the Director of National Intelligence, and shall remain sealed unless—
 - ''(1) an application for a court order with respect to the surveillance is made under section 104; or
 - ``(2) the certification is necessary to determine the legality of the surveillance under section 106(f).
- ''AUTHORIZATION FOR ACQUISITION OF FOREIGN
 INTELLIGENCE INFORMATION
- ''SEC. 102A. (a) IN GENERAL.—Notwithstanding any other law, the President, acting through 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 Attorney General certifies in writing under oath that the Attorney General has determined that—

- ''(1) the acquisition does not constitute electronic surveillance;
- ''(2) 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; ''(3) a significant purpose of the acquisition is to obtain foreign intelligence information; and ''(4) the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h).

- ''(b) SPECIFIC PLACE NOT REQUIRED.—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) SUBMISSION OF CERTIFICATION.—The Attorney General shall immediately transmit 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 102B.
- ''(d) MINIMIZATION PROCEDURES.—An acquisition under this section may be conducted only in accordance with the certification of the Attorney General and the minimization procedures adopted by the Attorney General. 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).

''DIRECTIVES RELATING TO ELECTRONIC SURVEILLANCE AND OTHER ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION ''SEC. 102B. (a) DIRECTIVE.—With respect to an authorization of electronic surveillance under section 102 or an authorization of an acquisition under section 102A, the Attorney General may direct a person to—

- ''(1) immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition of foreign intelligence information in such a manner as will protect the secrecy of the electronic surveillance or 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 electronic surveillance or acquisition or the aid furnished that such person wishes to maintain.
- ''(b) COMPENSATION.—The Government shall compensate, at the prevailing rate, a person for

providing information, facilities, or assistance pursuant to subsection (a).

- ''(c) FAILURE TO COMPLY.—In the case of a failure to comply with a directive issued pursuant to subsection (a), 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 (a) 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.
- ''(d) REVIEW OF PETITIONS.—(1) (A) A person receiving a directive issued pursuant to subsection (a) 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 24 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.
- "(e) APPEALS.—The Government or a person receiving a directive reviewed pursuant to subsection (d) may file a petition with the Court of Review established under section 103(b) for review of the decision issued pursuant to subsection (d) 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.
- ''(f) PROCEEDINGS.—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.

- ''(g) SEALED PETITIONS.—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.
- ''(h) LIABILITY.—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.
- ''(i) RETENTION OF DIRECTIVES AND ORDERS.—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.''.
- "USE OF INFORMATION ACQUIRED UNDER SECTION 102A
 "SEC. 102C. (a) USE OF INFORMATION.—Information
 acquired from an acquisition conducted pursuant to
 section 102A concerning any United States person may
 be used and disclosed by Federal officers and
 employees without the consent of the United States
 person only in accordance with the minimization
 procedures required by section 102A. No otherwise
 privileged communication obtained in accordance with,

or in violation of, the provisions of section 102A shall lose its privileged character. No information from an acquisition pursuant to section 102A may be used or disclosed by Federal officers or employees except for lawful purposes.

- ''(b) NOTIFICATION BY UNITED STATES.-Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against a person who was the target of, or whose communications or activities were subject to, an acquisition authorized pursuant to section 102A, any information obtained or derived from such acquisition, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to disclose or so use that information or submit it in evidence, notify such person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.
- ''(c) NOTIFICATION BY STATES OR POLITICAL SUBDIVISION.—Whenever any State or political

subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against a person who was the target of, or whose communications or activities were subject to, an acquisition authorized pursuant to section 102A, any information obtained or derived from such acquisition, the State or political subdivision thereof shall notify such person, the court, or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

"'(d) MOTION TO SUPPRESS.—(1) Any person against whom evidence obtained or derived from an acquisition authorized pursuant to section 102A is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress

the evidence obtained or derived from such acquisition on the grounds that—

- ''(A) the information was unlawfully
 acquired; or
- ''(B) the acquisition was not properly made in conformity with an authorization under section 102A.
- ''(2) A person moving to suppress evidence under paragraph (1) shall make the motion to suppress the evidence before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.
- "(e) IN CAMERA AND EX PARTE REVIEW BY DISTRICT
 COURT.—Whenever a court or other authority is notified
 pursuant to subsection (b) or (c) of this section, or
 whenever a motion is made pursuant to subsection (d)
 of this section, or whenever any motion or request is
 made pursuant to any other statute or rule of the
 United States or any State by a person who was the
 target of, or whose communications or activities were
 subject to, an acquisition authorized pursuant to
 section 102A before any court or other authority of
 the United States or any State—

- ''(1) to discover or obtain applications or orders or other materials relating to an acquisition authorized pursuant to section 102A, or
- ''(2) to discover, obtain, or suppress evidence or information obtained or derived from an acquisition authorized pursuant to section 102A, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the acquisition as may be necessary to determine whether such acquisition was lawfully authorized and conducted. In making this determination, the court may disclose to the person who was the target of, or whose communications or activities were subject to, an acquisition authorized pursuant to section 102A, under appropriate

security procedures and protective orders,
portions of the application, order, or other
materials relating to the acquisition only where
such disclosure is necessary to make an accurate
determination of the legality of the acquisition.

''(f) SUPPRESSION OF EVIDENCE; DENIAL OF MOTION.-If the United States district court, pursuant to subsection (e) of this section, determines that an acquisition authorized pursuant to section 102A was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from the acquisition or otherwise grant the motion of the person who was the target of, or whose communications or activities were subject to, an acquisition authorized pursuant to section 102A. If the court determines that such acquisition was lawfully authorized and conducted, it shall deny the motion of the person who was the target of, or whose communications or activities were subject to, an acquisition authorized pursuant to section 102A except to the extent that due process requires discovery or disclosure.

- ''(g) FINALITY OF ORDERS.—Orders granting motions or requests under subsection (f) of this section, decisions under this section that an acquisition was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to an acquisition shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.
- ''(h) CONSULTATION WITH LAW ENFORCEMENT

 OFFICERS.—(1). Federal officers who acquire foreign
 intelligence information pursuant to section 102A may
 consult with Federal law enforcement officers or law
 enforcement personnel of a State or political
 subdivision of a State (including the chief executive
 officer of that State or political subdivision who has
 the authority to appoint or direct the chief law
 enforcement officer of that State or political
 subdivision) to coordinate efforts to investigate or
 protect against—
 - ''(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

- ''(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
- ''(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.
- ''(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 102A.
- "(i) PROTECTIVE ORDERS AND PRIVILEGES.—Nothing in this section shall prevent the United States from seeking protective orders or asserting privileges ordinarily available to the United States to protect against the disclosure of classified information.".
- (b) 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 inserting after the item relating to section 102 the following:
 - ''102A. Authorization for acquisition of foreign intelligence information.
 - ''102B. Directives relating to electronic surveillance and other acquisitions of

foreign intelligence information.

"102C. Use of information acquired under section 102A."

SEC. 403. JURISDICTION OF FISA COURT.

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

- (1) in subsection (a), by inserting 'at least''
 before 'seven of the United States judicial
 circuits'; and
- (2) by adding at the end the following new subsection:
- ''(g) Applications for a court order under section 104 of this title are authorized if the Attorney General approves such applications to the court having jurisdiction under this section, and a judge to whom an application is made may, notwithstanding any other law, grant an order, in conformity with section 105, approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information.''.

SEC. 404. APPLICATIONS FOR COURT ORDERS.

Section 104 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804) is amended—

- (1) in subsection (a)-
 - (A) by striking paragraphs (2) and (11);
 - (B) by redesignating paragraphs (3) through (10) as paragraphs (2) through (9), respectively;
 - (C) in paragraph (5), as redesignated by
 subparagraph (B), by striking ''detailed
 description'' and inserting ''summary
 description'';
 - (D) in paragraph (6), as redesignated by subparagraph (B)-
 - (i) in the matter preceding subparagraph
 (A), by striking ''or officials designated''
 and all that follows through ''consent of
 the Senate'' and inserting ''designated by
 the President to authorize electronic
 surveillance for foreign intelligence
 purposes'';
 - (ii) in subparagraph (C), by striking
 ''techniques;'' and inserting ''techniques;
 and'';
 - (iii) by striking subparagraph (D); and

- (iv) by redesignating subparagraph (E) as subparagraph (D);
- (E) in paragraph (7), as redesignated by
 subparagraph (B), by striking 'a statement of
 the means' and inserting 'a summary statement
 of the means';
- (F) in paragraph (8), as redesignated by subparagraph (B)-
 - (i) by striking 'a statement' and
 inserting 'a summary statement'; and
 (ii) by striking 'application;' and
 inserting 'application; and'; and
- (G) in paragraph (9), as redesignated by subparagraph (B), by striking "; and" and inserting "."
- (2) by striking subsection (b);
- (3) by redesignating subsections (c) through (e) as subsections (b) through (d), respectively; and (4) in paragraph (1)(A) of subsection (d), as redesignated by paragraph (3), by striking 'or the Director of National Intelligence' and inserting 'the Director of National Intelligence, or the Director of the Central Intelligence Agency'.

SEC. 405. ISSUANCE OF AN ORDER.

Section 105 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805) is amended—

- (1) in subsection (a)-
 - (A) by striking paragraph (1); and
 - (B) by redesignating paragraphs (2) through (5) as paragraphs (1) through (4), respectively;
- (2) in paragraph (1) of subsection (c)-
 - (A) in subparagraph (D), by striking
 ''surveillance;'' and inserting ''surveillance;
 and'';
 - (B) in subparagraph (E), by striking 'approved;
 and' and inserting 'approved.'; and
 - (C) by striking subparagraph (F).
- (3) by striking subsection (d);
- (4) by redesignating subsections (e) through (i) as subsections (d) through (h), respectively;
- (5) in subsection (d), as redesignated by paragraph
 (4)-
- (A) by striking "120 days" and insert "one year", and
- (B) by amending paragraph (2) to read as follows:

 ''(2) Extensions of an order issued under this title

 may be granted on the same basis as an original order

upon an application for an extension and new findings made in the same manner as required for an original order and may be for a period not to exceed one year.'';

- (6) in subsection (e), as redesignated by paragraph(4), to read as follows:
- ''(e) Notwithstanding any other provision of this title, the Attorney General may authorize the emergency employment of electronic surveillance if the Attorney General—
- ''(1) determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained;
- ''(2) determines that the factual basis for issuance of an order under this title to approve such electronic surveillance exists;
- ''(3) informs a judge having jurisdiction under section 103 at the time of such authorization that the decision has been made to employ emergency electronic surveillance; and
- ''(4) makes an application in accordance with this title to a judge having jurisdiction under section 103

as soon as practicable, but not more than 168 hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes such emergency employment of electronic surveillance, the Attorney General shall require that the minimization procedures required by this title for the issuance of a judicial order be followed. In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 168 hours from the time of authorization by the Attorney General, which ever is earliest. In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United

States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information is significant foreign intelligence information or indicates a threat of death or serious bodily harm to any person. The Attorney General shall assess compliance with the requirements of the prior sentence and shall include such assessments in the Attorney General's reports under section 102(b). A denial of the application made under this subsection may be reviewed as provided in section 103.'';

- (7) in subsection (h), as redesignated by paragraph (4)-
 - (A) by striking 'a wire or' and inserting
 'an'; and
 - (B) by striking ''physical search'' and inserting ''physical search or in response to a certification by the Attorney General or a designee of the Attorney General seeking information, facilities, or technical assistance from such person under section 102B''; and
- (8) by adding at the end the following new subsection:

''(i) In any case in which the Government makes an application to a judge under this title to conduct electronic surveillance involving communications and the judge grants such application, upon the request of the applicant, the judge shall also authorize the installation and use of pen registers and trap and trace devices, and direct the disclosure of the information set forth in section 1842(d)(2) of this title; such information shall not be subject to minimization procedures.''.

SEC. 406. USE OF INFORMATION.

Section 106 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1806) is amended—

- (1) in subsection (i)-
- (A) by striking 'radio communication' and inserting 'communication'; and
- [(B) by striking 'contents indicates' and
 inserting 'contents contain significant foreign
 intelligence information or indicate'; and
- (2) by inserting after subsection (k) the following"]
- "(1) PROTECTIVE ORDERS AND PRIVILEGES.—Nothing in this section shall prevent the United States from seeking protective orders or asserting privileges ordinarily available to the United States to protect against the disclosure of classified information.".

SEC. 407. WEAPONS OF MASS DESTRUCTION.

- (a) DEFINITIONS.-
 - (1) Subsection (a)(4) of section 101 of the Foreign
 Intelligence Surveillance Act of 1978 (50 U.S.C.
 1801(a)(4)) is amended by inserting ''or the
 international proliferation of weapons of mass
 destruction'' after ''international terrorism''.
 (2) Subsection (b)(1) of such section (50 U.S.C.
 1801(b)(1)) is amended—
 - (A) in subparagraph (C), by striking ``; or'' and
 inserting ``;''; and
 - (B) by adding at the end the following new subparagraphs:
 - ''(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or
 - ''(F) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power; or''.
 - (3) Subsection (e)(1)(B) of such section (50 U.S.C.
 1801(e)(1)(B)) is amended by striking ''sabotage or
 international terrorism'' and inserting ''sabotage,

international terrorism, or the international proliferation of weapons of mass destruction''.

- (4) Subsection (1) of such section (50 U.S.C. 1801(1)) is amended to read as follows:
 - ''(1) 'Weapon of mass destruction' means—
 ''(1) any destructive device (as such term is defined in section 921 of title 18, United States Code) that is intended or has the capability to cause death or serious bodily injury to a significant number of people;
 - "(2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors;
 "(3) any weapon involving a biological agent, toxin, or vector (as those terms are defined in section 178 of title 18, United States Code); or "(4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.".

(b) USE OF INFORMATION. -

(1) Section 106(k)(1)(B) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1806(k)(1)(B)) is amended by striking ''sabotage or international

terrorism'' and inserting 'sabotage, international terrorism, or the international proliferation of weapons of mass destruction''.

(2) Section 305(k)(1)(B) of such Act (50 U.S.C.
1825(k)(1)(B)) is amended by striking ''sabotage or
international terrorism'' and inserting ''sabotage,
international terrorism, or the international
proliferation of weapons of mass destruction''.

SEC. 408. LIABILITY DEFENSE.

- (a) IN GENERAL.-Notwithstanding any other law, and in addition to the immunities, privileges, and defenses provided by any other source of law, no action shall lie or be maintained in any court, and no penalty, sanction, or other form of remedy or relief shall be imposed by any court or any other body, against any person for the alleged provision to an element of the intelligence community of any information (including records or other information pertaining to a customer), facilities, or any other form of assistance, during the period of time beginning on September 11, 2001, and ending on the date that is the effective date of this Act, in connection with any alleged classified communications intelligence activity that the Attorney General or a designee of the Attorney General certifies, in a manner consistent with the protection of State secrets, is, was, would be, or would have been intended to protect the United States from a terrorist attack. This section shall apply to all actions, claims, or proceedings pending on or after the effective date of this Act.
- (b) JURISDICTION.—Any action or claim described in subsection (a) that is brought in a State court shall be deemed to arise under the Constitution and laws of the

United States and shall be removable pursuant to section 1441 of title 28, United States Code.

- (c) DEFINITIONS.—In this section:
 - (1) INTELLIGENCE COMMUNITY.—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)).
 - (2) PERSON.—The term ''person'' has the meaning given the term in section 2510(6) of title 18, United States Code.

SEC. 409. AMENDMENTS FOR PHYSICAL SEARCHES.

- (a) APPLICATIONS.—Section 303 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1823) is amended—
 - (1) in subsection (a)-
 - (A) by striking paragraph (2);
 - (B) by redesignating paragraphs (3) through (9) as paragraphs (2) through (8), respectively;
 - (C) in paragraph (2), as redesignated by
 subparagraph (B), by striking ''detailed
 description'' and inserting ''summary
 description'';
 - (D) in paragraph (3)(C), as redesignated by
 subparagraph (B), by inserting "or is about to
 be" before "owned";
 - (E) in paragraph (6), as redesignated by subparagraph (B)-
 - (i) in the matter preceding subparagraph
 (A), by striking ''or officials'' and all
 that follows through ''consent of the
 Senate'' and inserting ''designated by the
 President to authorize physical searches for
 foreign intelligence purposes'';

- (ii) in subparagraph (C), by striking
 ''techniques;'' and inserting ''techniques;
 and'';
- (iii) by striking subparagraph (D);
- (iv) by redesignating subparagraph (E) as
 subparagraph (D); and
- (v) in subparagraph (D), as redesignated by
 clause (iv), by striking ''certifications
 required by subparagraphs (C) and (D)'' and
 inserting ''certification required by
 subparagraph (C)''; and
- (F) in paragraph (8), as redesignated by
 subparagraph (B), by striking 'a statement' and
 inserting 'a summary statement'; and
- (2) in subsection (d)(1)(A), by striking 'or the Director of National Intelligence' and inserting 'the Director of National Intelligence, or the Director of the Central Intelligence Agency'.
- (b) ORDERS.—Section 304 of such Act (50 U.S.C. 1824) is amended—
 - (1) in subsection (a)-
 - (A) by striking paragraph (1);
 - (B) by redesignating paragraphs (2) through (5) as paragraphs (1) through (4), respectively; and

- (C) in paragraph (2)(B), as redesignated by
 subparagraph (B), by inserting "or is about to
 be" before "owned";
- (2) in subsection (e), to read as follows:
- ''(e) Notwithstanding any other provision of this title, the Attorney General may authorize the emergency employment of a physical search if the Attorney General—
 - ''(1) determines that an emergency situation exists with respect to the employment of a physical search to obtain foreign intelligence information before an order authorizing such physical search can with due diligence be obtained;
 - ''(2) determines that the factual basis for issuance of an order under this title to approve such physical search exists;
 - ''(3) informs a judge having jurisdiction under section 103 at the time of such authorization that the decision has been made to employ an emergency physical search; and
 - ''(4) makes an application in accordance with this title to a judge having jurisdiction under section 103 as soon as practicable, but not more

than 168 hours after the Attorney General authorizes such physical search. If the Attorney General authorizes such emergency employment of a physical search, the Attorney General shall require that the minimization procedures required by this title for the issuance of a judicial order be followed. In the absence of a judicial order approving such physical search, the physical search shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 168 hours from the time of authorization by the Attorney General, whichever is earliest. In the event that such application for approval is denied, or in any other case where the physical search is terminated and no order is issued approving the physical search, no information obtained or evidence derived from such physical search shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or

UNCLASSIFIED

political subdivision thereof, and no information concerning any United States person acquired from such physical search shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information is significant foreign intelligence information or indicates a threat of death or serious bodily harm to any person. The Attorney General shall assess compliance with the requirements of the prior sentence and shall include such assessments in the Attorney General's reports under section 302(a)(2). A denial of the application made under this subsection may be reviewed as provided in section 103.′′.

- (c) CONFORMING AMENDMENTS.—The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is further amended—
 - (1) in section 304(a)(5), by striking ''303(a)(7)(E)'' and inserting ''303(a)(6)(E)''; and
 - (2) in section 305(k)(2), by striking ''303(a)(7)'' and inserting ''303(a)(6)''.

SEC. 410. AMENDMENTS FOR EMERGENCY PEN REGISTERS AND TRAP AND TRACE DEVICES.

- (a) Section 403 of the Foreign Intelligence Surveillance
 Act of 1978 (50 U.S.C. 1843) is amended—
- (1) in subsection (a)(2) by striking "48 hours" and inserting "168 hours"; and
- (2) in subsection (c)(1)(C) by striking "48 hours" and inserting "168 hours".

SEC. 411. MANDATORY TRANSFER FOR REVIEW.

- (a) IN GENERAL.—In any case before any court challenging the legality of a classified communications intelligence activity relating to a foreign threat, or in which the legality of any such activity is in issue, if the Attorney General files an affidavit under oath that the case should be transferred to the Foreign Intelligence Surveillance Court because further proceedings in the originating court would harm the national security of the United States, the originating court shall transfer the case to the Foreign Intelligence Surveillance Court for further proceedings under this section.
- (b) PROCEDURES FOR REVIEW.—The Foreign Intelligence
 Surveillance Court shall have jurisdiction as appropriate
 to determine standing and the legality of the
 communications intelligence activity to the extent
 necessary for resolution of the underlying case. All
 proceedings under this paragraph shall be conducted in
 accordance with the procedures set forth in section 106(f)
 of the Foreign Intelligence Surveillance Act of 1978,
 except that the Foreign Intelligence Surveillance Court
 shall not require the disclosure of national security
 information to any person without the approval of the

Director of National Intelligence or the Attorney General, unless in the context of a criminal proceeding, disclosure would be constitutionally required. Any such constitutionally required disclosure shall be governed by the Classified Information Procedures Act, Pub. L. No. 96-456, 94 Stat. 2025 (1980), or if applicable, Title 18, United States Code, Section 2339B(f).

- (c) APPEAL, CERTIORARI, AND EFFECTS OF DECISIONS.—The decision of the Foreign Intelligence Surveillance Court made under paragraph (b), including a decision that the disclosure of national security information is constitutionally required, shall be subject to review by the Court of Review established under section 103(b) of the Foreign Intelligence Surveillance Act. The Supreme Court of the United States shall have jurisdiction to review decisions of the Court of Review by writ of certiorari granted upon the petition of the United States. The decision by the Foreign Intelligence Surveillance Court shall otherwise be binding in all other courts.
- (d) DISMISSAL.—The Foreign Intelligence Surveillance Court or a court that is an originating court under paragraph (a) may dismiss a challenge to the legality of a classified communications intelligence activity for any reason provided for under law.

(e) PRESERVATION OF LITIGATION PRIVILEGES.—All litigation privileges shall be preserved in the originating court and in the Foreign Intelligence Surveillance Court, the Foreign Intelligence Court of Review, and the Supreme Court of the United States, in any case that is transferred and received under this section.

SEC. 412. TECHNICAL AND CONFORMING AMENDMENTS.

The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is further amended—

- (1) in section 103(e)-
 - (A) in paragraph (1), by striking ``501(f)(1)'' and inserting ``102B(d) or 501(f)(1)''; and
 - (B) in paragraph (2), by striking ``501(f)(1)'' and inserting ``102B(d) or 501(f)(1)'';
- (2) in section 105-
 - (A) in subsection (a)(4), as redesignated by section 105(1)(B)—
 - (i) by striking ``104(a)(7)(E)'' and inserting ``104(a)(6)(D)''; and(ii) by striking ``104(d)'' and inserting
 - (B) in subsection (c)(1)(A), by striking ''104(a)(3)'' and inserting ''104(a)(2)'';
- (3) in section 106-

``104(c)'';

- (A) in subsection (j), in the matter preceding
 paragraph (1), by striking ``105(e)'' and
 inserting ``105(d)''; and
- (B) in subsection (k)(2), by striking
 ''104(a)(7)(B)'' and inserting ''104(a)(6)(B)'';
 and

(4) in section 108(a)(2)(C), by striking ''105(f)'' and inserting ''105(e)''.

SEC. 413. EFFECTIVE DATE.

- (a) Except as otherwise provided, the amendments made by this Act shall take effect 90 days after the date of the enactment of this Act.
- (b) 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)) may 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 court established under section 103(a) of such Act shall extinguish any such order at the request of the applicant.

SEC. 414. CONSTRUCTION; SEVERABILITY.

Any provision of this Act held to be invalid or unenforceable by its terms, or as applied to any person or circumstance, shall be construed so as to give it the maximum effect permitted by law, unless such holding shall be one of utter invalidity or unenforceability, in which event such provision shall be deemed severable from this Act and shall not affect the remainder thereof or the application of such provision to other persons not similarly situated or to other, dissimilar circumstances.

FISA MODERNIZATION PROVISIONS OF THE PROPOSED FISCAL YEAR 2008 INTELLIGENCE AUTHORIZATION

SECTIONAL ANALYSIS

Sec. 400. Short title.

This section sets forth the title of this portion of the bill as the ''Foreign Intelligence Surveillance Modernization Act of 2007''.

Sec. 401. Definitions.

Section 401 amends the definitions of several terms used in the Foreign Intelligence Surveillance Act (FISA) $(50\ U.S.C.\ 1801-1871)$.

Subsection 401(a) amends FISA's definition of "agent of a foreign power" to include non-U.S. persons who possess or receive <u>significant</u> foreign intelligence information while in the United States. This amendment fills a gap in FISA's current definition to address circumstances in which a foreign individual is known to have valuable foreign intelligence information, but the individual's relationship to a foreign power is unclear. Collection of information from such an individual would be subject to the approval of the Foreign Intelligence Surveillance Court (FISC).

Subsection 401(b) also amends FISA's definition of "electronic surveillance." When FISA was enacted in 1978, Congress used language that was technology-dependent and related specifically to the telecommunications systems that existed 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 intended to exclude from FISA's scope. Subsection 401(b) provides a new, technologically 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 mean: "(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." addition to enhancing our intelligence capabilities, this change would advance the privacy rights of Americans, as it would focus the resources of the FISC and the Government on

the review of applications to conduct surveillance that most directly implicate the privacy interests of persons in the United States. This would restore FISA to its original focus and would do so in a way that no longer depends on unforeseeable technological changes.

Additionally, section 401 strikes FISA's current definition of "wire communication". Reference to this term is unnecessary under the new technologically neutral definition of "electronic surveillance".

Section 401 also amends the definition of the term "minimization procedures." This amendment is intended to conform the definition to changes to be made to subsection 102(a) of FISA.

Additionally, section 401 amends the definition of the term "contents" to make that definition consistent with the definition of the same term in Title III (18 U.S.C. 2510), which pertains to interception of communications in criminal investigations. This change would address an inconsistency between subchapter III of FISA (pertaining to pen registers and trap and trace devices) and subchapter I of FISA (pertaining to electronic surveillance). Currently, the definitions of the terms "pen register" and "trap and trace device" in subchapter III of FISA incorporate the definitions provided in 18 U.S.C. 3127. Those definitions, in turn, use the term "contents," which is defined under Title III (18 U.S.C. 2510) to include "any information concerning the substance, purport, or meaning" of a communication. Section 401 would apply this definition of "contents," which Congress already has incorporated into subchapter III of FISA, to the rest of the statute. This change would therefore remove ambiguity from the current definitions.

Sec. 402. Attorney General Authorization for Electronic Surveillance.

Section 402 amends section 102 of FISA (50 U.S.C. 1802).

With regard to foreign intelligence targets located within the United States, section 402 alters the circumstances in which the Attorney General can exercise his authority to authorize electronic surveillance without a court order under section 102 of FISA. Currently, subsection 102(a) 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. Changes in communications technology and practices have seriously eroded the usefulness of the current version.

Importantly, this amendment does not change the types of "foreign powers" to which this authority applies nor does it change the handling of incidental information concerning U.S. persons. Any communications involving U.S. persons that are intercepted will be handled in accordance with minimization procedures that are equivalent to those that govern Court-ordered collection.

Section 402 also adds new procedures (section 102A) 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. An acquisition under new section 102A must involve obtaining foreign intelligence information from or with the assistance of a communications provider, custodian, or other person who has access to such communications. Appropriate minimization procedures also must be followed.

Finally, Section 402 provides the means through which the Attorney General can compel cooperation with authorizations made under the amended 102(a) or 102A as well as procedures governing the use of information gathered pursuant to section 102A. These are found in section 102B and 102C, respectively. Presently, the Attorney General is authorized to direct a communications

carrier to assist the government with the exercise of electronic surveillance authorized under section 102(a). However, FISA does not currently provide a means by which the Attorney General can seek court assistance to compel compliance with a directive or for recipients of such directives to challenge them in court. The new procedures remedy these deficiencies.

Sec. 403. Jurisdiction of FISA Court.

Section 403 amends section 103 of FISA (50 U.S.C. 1803).

Subsection 403(a) amends section 103(a) to provide that judges on the FISC shall be drawn from "at least seven" of the United States judicial circuits, rather than the current requirement that judges be drawn from seven of the circuits.

Subsection 403(b) moves (with minor amendments) a provision that currently appears in section 102 to the section that pertains to the jurisdiction of the FISC.

Sec. 404. Applications for Court Orders.

The current procedure for applying to the FISC for a surveillance order under section 104 of FISA (50 U.S.C. 1804) should be streamlined. Currently, the government has to provide significant amounts of information that serves little or no purpose in safeguarding civil liberties. Section 404 streamlines the FISA application process to increase the efficiency of the process while still providing the FISC the information it needs in considering whether to authorize the surveillance. For example, subsection 404(1) amends the current FISA provisions requiring that the application contain a "detailed description of the nature of the information sought," and allows the government to submit a summary description of such information. Subsection 404(1) similarly amends the current requirement that the application contain a "statement of facts concerning all previous applications" involving the target, and instead permits the government to provide a summary of those facts.

Section 404 also would allow FISA certifications to be made by individuals specifically designated by the President. This change would help resolve a current bottleneck in the FISA process caused by the fact that few officials currently can certify FISA applications. In view of the requirement of a presidential designation, civil liberties still would be protected.

Sec. 405. Issuance of an Order.

Section 405 amends the procedures for the issuance of an order under section 105 of FISA (50 U.S.C. 1805) to conform with the changes to the application requirements that would be effected by changes to section 104. It also would extend the initial term of authorization for electronic surveillance of a non-U.S. person who is an agent of a foreign power from 120 days to one year. This change will reduce time spent preparing applications for renewals relating to non-U.S. persons thereby allowing more resources to be devoted to cases involving U.S. persons.

Additionally, subsection 405(6) amends the procedures for the emergency authorization of electronic surveillance without a court order, to allow the Executive Branch seven days to obtain court approval after surveillance is initially authorized by the Attorney General. (The current period is 72 hours.) This change will help ensure that the Executive Branch has sufficient time in an emergency situation to 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. Subsection 405(6) also would allow for the retention of information if it "contains significant foreign intelligence information."

Subsection 405(8) also adds a new paragraph that requires the FISC, when granting an application for electronic surveillance, to simultaneously authorize the installation and use of pen registers and trap and trace devices if requested by the government. This change merely saves paperwork, as the standard to obtain a court order for electronic surveillance is substantially higher than the pen-register standard.

Sec. 406. Use of Information.

Section 406 amends subsection 106(i) of FISA (50 U.S.C. 1806(i)) which pertains to limitations regarding the use of unintentionally acquired information. Currently, subsection 106(i) provides that unintentionally acquired radio communications between persons located in the United States be destroyed unless the Attorney General determines that the communications indicate a threat of death or serious bodily harm. Section 406 amends subsection 106(i) by making it technology neutral - the same rule should apply no matter how the communication is transmitted. [It would also allow for the retention of 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. 1

Section 406 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.

Sec. 407. Weapons of Mass Destruction.

Section 407 amends sections 101, 106, and 305 of FISA (50 U.S.C. 1801, 1806, 1825) to address weapons of mass destruction. These amendments reflect the threat posed by these catastrophic weapons and extend FISA to apply to individuals and groups engaged in the international proliferation of such weapons.

Subsection 407(a) amends section 101 of FISA to include a definition of the term "weapon of mass destruction." Subsection 407(a) also amends the section 101 definitions of "foreign power" and "agent of a foreign power" to include groups and individuals engaged in the international proliferation of weapons of mass destruction. Subsection 407(a) similarly amends the definition of "foreign intelligence information."

Subsection 407(b) also amends sections 106 and 305 of FISA to cover the use of information regarding international proliferation of weapons of mass destruction.

Sec. 408. Liability Defense.

Telecommunications providers who are alleged to have assisted the government with intelligence activities after September 11th have faced numerous lawsuits as a result of their alleged activities in support of the government's efforts to prevent another terrorist attack. Companies that cooperate with the Government in the war on terror deserve our appreciation and protection – not litigation. This provision would protect providers from liability based upon allegations that they assisted the government in connection with alleged classified communications intelligence activities intended to protect the United States from a terrorist attack since September 11, 2001. Section 408 also provides for the removal of any such actions from state to federal court.

Sec. 409. Amendments for Physical Searches.

Section 409 amends section 303 of FISA (50 U.S.C. 1823) to streamline the application process for physical searches, update and augment the emergency authorization provisions, and increase the potential number of officials who can certify FISA applications. These changes parallel those proposed to the electronic surveillance application process.

Sec. 410. Amendments for Emergency Pen Registers and Trap and Trace Devices.

Section 410 amends the FISA section 403 (50 U.S.C. 1843) procedures 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.

Sec. 411. Mandatory Transfer for Review.

Section 411 would allow for the transfer of sensitive national security litigation to the Foreign Intelligence Surveillance Court. This provision requires courts to transfer a case to the FISC 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 FISC, section 411 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 411 also provides that the decisions of the FISC 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.

Additionally, section 411 provides that all litigation privileges are preserved in the originating court, the FISC, the FISA Court of Review, and the Supreme Court of the United States, in any case transferred under that section.

Sec. 412. Technical and Conforming Amendments.

Section 412 makes technical and conforming amendments to sections 103, 105, 106, and 108 of FISA (50 U.S.C. 1803, 1805, 1806, 1808).

Sec. 413. Effective Date.

Section 413 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 also allow for a smooth transition after the changes take effect.

Sec. 414. Construction; Severability.

Section 414 provides that any provision in sections 401 through 414 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.