Order Code RL33637

CRS Report for Congress
Received through the CRS Web

H.R. 5825 (109th Congress): "Electronic Surveillance Modernization Act"

September 8, 2006

Elizabeth B. Bazan
Legislative Attorney
American Law Division

GalleryWatch.com
http://www.crsdocuments.com
Penny Hill Press

H.R. 5825 (109th Congress): "Electronic Surveillance Modernization Act"

Summary

In discussing the need for the National Security Agency's "Terrorist Surveillance Program," a program in which international communications of persons within the United States have been the subject of electronic surveillance without a warrant or a Foreign Intelligence Surveillance Court order, where one party to the communication is believed to be a member of al Qaeda, affiliated with al Qaeda, a member of an organization affiliated with al Qaeda, or working in support of al Qaeda, the Bush Administration has stated that electronic surveillance under the Foreign Intelligence Surveillance Act (FISA), while still a valuable tool in combating terrorism, lacks the speed and agility to deal with such terrorists or terrorist groups. Critics have challenged the NSA program on legal and constitutional grounds. On August 17, 2006, in *American Civil Liberties Union v. National Security Agency*, Case No. 06-CV-10204 (E.D. Mich. August 17, 2006), U.S. District Court Judge Anna Diggs Taylor held the program unconstitutional on the ground that it violated the Administrative Procedures Act, the Separation of Powers doctrine, the First and Fourth Amendments of the U.S. Constitution, the Foreign Intelligence Surveillance Act (FISA), and Title III of the Omnibus Crime Control and Safe Streets Act (Title III). The decision has been appealed.

Several bills have been introduced in the House of Representatives and in the Senate to amend the Foreign Intelligence Surveillance Act and to address questions raised with respect to the "Terrorist Surveillance Program." H.R. 5825, the "Electronic Surveillance Modernization Act," was introduced on July 18, 2006. The bill was referred on that date to both the House Committee on the Judiciary and to the House Permanent Select Committee on Intelligence. On September 1, 2006, it was referred to the Subcommittee on Crime, Terrorism, and Homeland Security of the House Judiciary Committee. H.R. 5825 was one of several bills that were the focus of a hearing held before the House Judiciary Committee's Subcommittee on Crime, Terrorism, and Homeland Security on Wednesday, September 6, 2006. This report will summarize the provisions of the bill and discuss the impact of its provisions, if passed, on current law.

Contents

Introduction 1

Sec. 2. FISA Definitions 3

Sec. 3. Authorization for Electronic Surveillance for Foreign Intelligence Purposes 8

Sec. 4. Applications for Court Orders 9

Sec. 5. Issuance of an Order 13

Sec. 6. Use of Information 17

Sec. 7. Authorization after an Armed Attack 18

Sec. 8. Authorization of Electronic Surveillance after a Terrorist Attack 18

Sec. 9. Congressional Oversight 20

Sec. 10. Technical and Conforming Amendments 22

Penny Hill Press
http://www.crsdocuments.com
GalleryWatch.com

H.R. 5825 (109th Congress): "Electronic Surveillance Modernization Act"

Introduction

In discussing the need for the National Security Agency's "Terrorist Surveillance Program," a program in which international communications of persons within the United States have been the subject of electronic surveillance, without a warrant or a Foreign Intelligence Surveillance Court (FISC) order, where one party to the communication is believed to be a member of al Qaeda, affiliated with al Qaeda, a member of an organization affiliated with al Qaeda, or working in support of al Qaeda, the Bush Administration has stated that electronic surveillance under the Foreign Intelligence Surveillance Act, while still a valuable tool in combating terrorism, lacks the speed and agility needed to deal with such terrorists or terrorist groups.[1] The Foreign Intelligence Surveillance Act (FISA), P.L. 95-511, Title I, October 25, 1978, 92 Stat. 1796, codified at 50 U.S.C. § 1801 *et seq.*, as amended, provides a statutory framework for the use of electronic surveillance, physical searches, pen registers and trap and trace devices to acquire foreign intelligence information.[2] It also provides statutory authority for the production of tangible things

---

[1] *See* U.S. DEPARTMENT OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT 34 (January 19, 2005); Letter of December 22, 2005, from Assistant Attorney General William E. Moschella to the Honorable Pat Roberts, the Honorable John D. Rockefeller, IV, the Honorable Peter Hoekstra, and the Honorable Jane Harman, at 5; Statements by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, during December 19, 2005, Press Briefing available at [http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html].

[2] Under section 101(e) of FISA, 50 U.S.C. § 1801(e), "foreign intelligence information" is defined to mean:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to 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 or international terrorism 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; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to —
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

(continued...)

for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.[3] Several bills have been introduced in the House of Representatives and in the Senate to amend the Foreign Intelligence Surveillance Act and to address concerns raised with respect to the "Terrorist Surveillance Program."

H.R. 5825, the "Electronic Surveillance Modernization Act," was introduced on July 18, 2006, by Representative Heather Wilson, for herself, Representative Sensenbrenner, Representative Hoekstra, Representative Renzi, Representative Johnson of Connecticut, Representative Everett, Representative Thornberry, Representative Rogers of Michigan, Representative Gallegly and Representative Issa. The bill was referred the same day to both the House Committee on the Judiciary and to the House Permanent Select Committee on Intelligence. On September 1, 2006, it was referred to the Subcommittee on Crime, Terrorism, and Homeland Security of the House Judiciary Committee. H.R. 5825 was one of several bills[4] that were the focus of a hearing before the Subcommittee on Crime, Terrorism, and Homeland Security of the House Judiciary Committee on Wednesday, September 6, 2006. This report will summarize the provisions of H.R. 5825 and will discuss the impact of its provisions, if passed, on current law. The sections of the bill will be addressed in the order in which they appear in the bill.

---

[2] (...continued)
"International terrorism" is defined in subsection 101(c), 50 U.S.C. § 1801(c) to mean activities that:

> (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
> (2) appear to be intended —
> (A) to intimidate or coerce a civilian population;
> (B) to influence the policy of a government by intimidation or coercion; or
> (C) to affect the conduct of a government by assassination or kidnapping; and
> (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

"Sabotage" is defined in 50 U.S.C. § 1801(d) to mean "activities that involve a violation of chapter 105 of Title 18, or that would involve such a violation if committed against the United States."

[3] Under Sec. 106(a)(1) of FISA, 50 U.S.C. § 1861(a)(1), where such an investigation is of a United States person, it may not be conducted "solely upon the basis of activities protected by the first amendment to the Constitution."

[4] The Subcommittee hearing was on "Legislative Proposals to Update the Foreign Intelligence Surveillance Act (FISA)." The bills anticipated to be considered were H.R. 4976, H.R. 5223, H.R. 5371, H.R. 5825, S. 2453, and S. 2455.

Sec. 2. FISA Definitions

Sec. 2 of the bill amends the current definitions in the Foreign Intelligence Surveillance Act (FISA). Sec. 2(a) amends definition of "agent of a foreign power" in subsection 101(b)(1), 50 U.S.C. § 1801(b)(1),[5] to add a new category covering any person, other than a United States person,[6] who "(D) possesses or is reasonably expected to transmit or receive foreign intelligence information while in the United States." Unlike the definitions of "agent of a foreign power" in subsections 101(b)(1)(A) and 101(b)(1)(B), but like the so-called "lone wolf" provision in subsection 101(b)(1)(C), the definition of an "agent of a foreign power" under proposed subsection 101(b)(1)(D) does not require that the non-U.S. person covered by this new definition have any connection with a foreign power. However, it differs from the latter provision in that under proposed subsection 101(b)(1)(D), possession of foreign intelligence information by a non-U.S. person, without more, appears sufficient for that person to be categorized as an "agent of a foreign power." Alternatively, under the proposed new definition, a non-U.S. person who is "reasonably expected to transmit or receive foreign intelligence information while in the United States" would also be considered an "agent of a foreign power." The proposed definition does not appear to require an action or intent to act for the benefit of a foreign power or against the interests of the United States, nor does it require any ill intent. This would seem to significantly broaden the reach of the term so defined.

Sec. 2(b) amends the definition of "electronic surveillance" in subsection 101(f) of FISA, 50 U.S.C. § 1801(f), to mean:

---

[5] Under current law, "agent of a foreign power" under section 101(b)(1) of FISA, 50 U.S.C. § 1801(b)(1) includes three categories of persons, who are not United States persons. These categories include any person other than a United States person, (A) who acts in the United States as an officer or employee of a foreign power, or, as a member of a group engaged in international terrorism or activities in preparation therefor; (B) who acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or (C) who engages in international terrorism or activities in preparation for international terrorism.

[6] Under section 101(i) of FISA, 50 U.S.C. § 1801(i), a "United States person" is defined to mean "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act [8 U.S.C. § 1101(a)(20)]), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section." Under the cross-referenced sections, "foreign power" means "a foreign government or any component thereof, whether or not recognized by the United States;" "a faction of a foreign nation or nations, not substantially composed of United States persons;" or "an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments." It does not include international terrorist organizations.

> (1) the installation or use of a surveillance device [as defined in subsection (2)(d) of the bill, new subsection 101(*l*) of FISA, 50 U.S.C. § 1801(*l*)[7]] for the intentional collection of information relating to a person who is reasonably believed to be in the United States by intentionally targeting that person, under circumstances in which the 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, without the consent of a party to the communication, under circumstances in which a person has reasonable expectation of privacy and a warrant would be required for law enforcement purposes, if both the sender and all intended recipients are located within the United States.[8]

Although this is a broader, shorter, and more general definition than that contained in current law, there are some similarities in language.

Proposed subsection 101(f)(1) blends some of the elements of current subsections 101(f)(1) and (f)(4) with new elements, while eliminating other aspects

---

[7] Under current law, section 101(*l*) of FISA, 50 U.S.C. § 1801(l) defines "wire communication" to mean, "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications." Under the new definition of "surveillance device" in Sec. 2(d) of H.R. 5825, the term would mean, "a device that allows surveillance by the Federal Government, but excludes any device that extracts or analyzes information from data that has already been acquired by the Federal Government by lawful means." While the term "surveillance device" is not currently defined in FISA, it is used in the current definition of "electronic surveillance" under subsection 101(f) of FISA, 50 U.S.C. § 1801(f).

[8] Under current law, "electronic surveillance" is defined under subsection 101(f) of FISA, 50 U.S.C. § 1801(f), to mean:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;
> (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

of those provisions. Current subsection 101(f)(1) deals with the use of a surveillance device to intercept the contents of wire or radio communications sent by or intended to be received by a particular, known, intentionally targeted U.S. person, who is in the United States, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. Current subsection 101(f)(4) deals with the installation or use of a surveillance device in the United States "for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." However, unlike current subsection 101(f)(1), the new definition does not explicitly distinguish between interception of the communications of U.S. persons and those of non-U.S. persons, nor is it restricted to acquisition of the contents of communications. The current subsection 101(f)(1) requires the person intentionally targeted to be in the United States, while the proposed provision requires a reasonable belief that the intentionally targeted person be in the United States. While both proposed subsection 101(f)(1) and current subsection 101(f)(4) deal with the installation or use of a surveillance device to acquire information, unlike current subsection 101(f)(4), the proposed definition contains no express requirement that the surveillance device be installed or used in the United States, and no restriction on acquisition of that information from wire or radio communications. The proposed subsection 101(f)(1) explicitly involves intentional targeting of a person, while current subsection 101(f)(4) does not.

New subsection 101(f)(2) has significant parallels to current subsection 101(f)(3), in that both deal with "intentional acquisition" of the contents of a "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 the intended recipients are located in the United States." However, the current provision is limited to intentional acquisition of radio communications by means of "an electronic, mechanical, or other surveillance device," and does not include a requirement that the interception be "without the consent of any party to the communication." Consent is addressed in current subsection 101(f)(2), which deals with acquisition, rather than intentional acquisition, within the United States, of a communication to or from a person in the United States, without that party's consent. The latter provision exempts from coverage "the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18." Proposed subsection 101(f)(2) contains no similar exemption.

Under current law, "minimization procedures" are defined in section 101(h) of FISA, 50 U.S.C. § 1801(h)(1)-(4). Sec. 2(c) of H.R. 5825 amends the definition of "minimization procedures" in section 101(h), 50 U.S.C. § 1801(h), to delete subsection (4). Current Section 101(h)(4) of FISA, 50 U.S.C. § 1801(h)(4), includes in the definition of "minimization procedures," with respect to any electronic surveillance approved pursuant to 50 U.S.C. § 1802(a), "procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person."

Under the current section 102(a) of FISA, 50 U.S.C. § 1802(a), the President, through the Attorney General, may authorize electronic surveillance without a court order under FISA to acquire foreign intelligence information for periods of up to one year based upon a written certification under oath by the Attorney General that meets certain criteria and satisfies specified reporting requirements. Under these criteria, the Attorney General must certify that the electronic surveillance is solely directed at either the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 101(a)(1), (2) or (3) of FISA, 50 U.S.C. § 1801(a)(1), (2), or (3); or the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as so defined. Under the cross-referenced sections, "foreign power" means a foreign government or any component thereof, whether or not recognized by the United States; a faction of a foreign nation or nations, not substantially composed of United States persons; or an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments. It does not include international terrorist organizations. As amended by Sec. 3(1)(A) of H.R. 5825, discussed *infra*, subsection 102(a)(1) would also cover acquisition of the contents of communications of an "agent of a foreign power" as defined in section 101(b)(1) of FISA, 50 U.S.C. § 1801(b)(1), which deals with agents of foreign powers who are not U.S. persons.

In addition, current law requires the Attorney General, when acting under section 102 of FISA, 50 U.S.C. § 1802, to certify that there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party. As amended by Sec. 3 of H.R. 5825, this requirement would be eliminated. Current law also requires the Attorney General, in authorizing electronic surveillance without a court order under Section 102 of FISA, to certify that the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 101(h) of FISA, 50 U.S.C. § 1801(h).

Under current subsection 102(a) of FISA, 50 U.S.C. § 1802(a), also requires the Attorney General to report such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately.

Under current subsection 102(a)(2) of FISA, 50 U.S.C. § 1802(a)(2), an electronic surveillance authorized by this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures adopted by him. The Attorney General is required to assess compliance with the minimization procedures and to report such assessments to the House

Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence under the provisions of section 108(a) of FISA, 50 U.S.C. §1808(a).[9]

Sec. 2(d) of the bill replaces current definition of "wire communication" in section 101(*l*) with a definition of "surveillance device," which means "a device that allows surveillance by the Federal Government, but excludes any device that extracts or analyzes information from data that already has been acquired by the Federal Government by lawful means."[10]

Sec. 2(e) of H.R. 5825 amends subsection 301(5) of FISA, 50 U.S.C. § 1821(5), which currently defines "physical search" to mean

> any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, but does not include (A) "electronic surveillance", as defined in section 101(f) of this Act [1801(f) of this title], or (B) the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101(f) of this Act [1801(f) of this title].

---

[9] Under current section 102(a)(3) of FISA, 50 U.S.C. § 1802(a)(3), the Attorney General is required to immediately transmit his certification under seal to the Foreign Intelligence Surveillance Court, which would remained sealed unless (A) an application for a court order with respect to the surveillance is made under sections 101(h)(4) of FISA, 50 U.S.C. § 1801(h)(4) and section 104 of FISA, 50 U.S.C. § 1804; or (B) the certification is necessary to determine the legality of the surveillance under section 106(f) of FISA, 50 U.S.C. § 1806(f). As amended by Sec. 10(1) of H.R. 5825, the reference to 101(h)(4) of FISA, 50 U.S.C. § 1801(h)(4), in subsection 102(a)(3)(A), 50 U.S.C. § 1802(a)(3)(A) would be deleted. It may be noted that, as so amended, the "sections" which currently precedes this reference would remain plural.

Pursuant to current section 102(a)(4) of FISA, 50 U.S.C. § 1802(a)(4), in regard to electronic surveillance authorized by Section 102(a), the Attorney General may direct a specified communication carrier to "(A) furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers;" and "(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the surveillance or the aid furnished which such carrier wishes to retain." The Government is also directed to compensate the communications carrier at the prevailing rate for furnishing such aid. Section 3(2) of H.R. 5825 would strike Section 102(a)(4) of FISA, 50 U.S.C. § 1802(a)(4).

[10] For further discussion of these definitions, see footnote 4, *supra*.

Sec. 2(e) amends definition of "physical search" in subsection 301(5) of FISA, 50 U.S.C. § 1821(5), to include activities described in section 102(b) of FISA, 50 U.S.C. § 1802(b), as amended by Sec. 3 of the bill.[11]

Sec. 3. Authorization for Electronic Surveillance for Foreign Intelligence Purposes

Sec. 3 of H.R. 5825 amends section 102 of FISA, 50 U.S.C. § 1802. Sec. 3(1)(A) amends subsection 102(a)(1)(A)(i) to cover acquisition of the contents of communications of a "foreign power," as defined in section 101(a)(1), (2), or (3) of FISA, 50 U.S.C. § 1801(a)(1), (2), or (3) (that is, a foreign government or any component thereof, whether or not recognized by the United States; a faction of a foreign nation or nations, not substantially composed of United States persons; or an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments); or an "agent of a foreign power" as defined in section 101(b)(1) (that is, an agent of a foreign power who is not a U.S. person).

Sec. 3(1)(B) deletes subsection 102(a)(1)(B) of FISA, 50 U.S.C. § 1802(a)(1)(B) and redesignates subparagraph 102(a)(1)(C) of FISA as subparagraph 102(a)(1)(B) of FISA. Under current law, subsection 102(a)(1)(B) of FISA requires the Attorney General, in authorizing electronic surveillance without a court order under section 102 of FISA, 50 U.S.C. § 1802, to certify that "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party."

Sec. 3(2) deletes subsection 102(a)(4) of FISA, 50 U.S.C. § 1802(a)(4). Pursuant to current subsection 102(a)(4) of FISA, 50 U.S.C. § 1802(a)(4), with respect to electronic surveillance authorized by subsection 102(a) of FISA, 50 U.S.C. § 1802(a), the Attorney General may direct a specified communication carrier to "(A) furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers;" and "(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the surveillance or the aid furnished which such carrier wishes to retain." The Government is also directed to compensate the communications carrier at the prevailing rate for furnishing such aid.

---

[11] Under Sec. 2(e) of H.R. 5825, subsection 301(5), 50 U.S.C. § 1801(5) would be amended by replacing "Act , or (B)" with "Act, (B) activities described in Section 102(b) of this Act, or (C)."

Sec. 3(3) amends subsection 102(b)[12] of FISA, 50 U.S.C. § 1802(b), to authorize the Attorney General to require, by written certification, any person with authorized access to electronic communications or equipment used to transmit or store electronic communications to provide information, facilities, or technical assistance necessary to accomplish electronic surveillance authorized under subsection 102(a); or to provide such information, facilities, or technical assistance to an official designated by the President for up to one year, provided the Attorney General certifies in writing, under oath, that the provision of the information, facilities, or technical assistance does not constitute electronic surveillance. As amended, subsection 102(b) of FISA, 50 U.S.C. § 1802(b) would also provide that the Attorney General may require a person providing such information, facilities, or technical assistance to do so in such a manner as to protect the secrecy of such provision of information, facilities or technical assistance and produce a minimum of interference with customer services; and may require such person to maintain any records he or she wishes to retain concerning such electronic surveillance or the information, facilities, or technical assistance provided, under security procedures approved by the Attorney General and the Director of National Intelligence (DNI). In addition, the new subsection 102(b) of FISA would authorize compensation by the Government to a person providing information, facilities, or technical assistance at the prevailing rate.

Sec. 3(4) of H.R. 5825 would add a new subsection 102(c) to FISA, new 50 U.S.C. § 1802(c), stating, "Notwithstanding any other provision of law, the President may designate an official who may authorize electronic surveillance of international radio communications of a diplomat or diplomatic mission or post of the government of a foreign country in the United States in accordance with procedures approved by the Attorney General."

Sec. 4. Applications for Court Orders

Sec. 4 of H.R. 5825 amends section 104 of FISA, 50 U.S.C. § 1804, dealing with applications for court orders for electronic surveillance. The new language would:

---

[12] Current subsection 102(b) of FISA, 50 U.S.C. § 1802(b) provides:

> (b) Applications for a court order under this subchapter are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the court having jurisdiction under section 103 [1803 of this title], and a judge to whom an application is made may, notwithstanding any other law, grant an order, in conformity with section 105 [1805 of this title], approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information, except that the court shall not have jurisdiction to grant any order approving electronic surveillance directed solely as described in paragraph (1)(A) of subsection (a) of this section unless such surveillance may involve the acquisition of communications of any United States person.

- under Sec. 4(1)(A) of the bill, strike the requirements in subsections 104(a)(6), (9), and (11) of FISA, 50 U.S.C. §§ 1804(a)(6), (9), and (11),[13] thereby eliminating three categories of information currently required to be included in applications for FISC orders authorizing electronic surveillance for foreign intelligence purposes.

- under Sec. 4(1)(B) of the bill, redesignate subsections 104(a)(7), (8) and (10) of FISA, 50 U.S.C. §§ 1804(a)(7), (8), and (10), as subsections 104(a)(6), (7) and (8), 50 U.S.C. §§ 1804(a)(6), (7), and (8).

- under Sec. 4(1)(C)(i) of the bill, amend the introductory language in the newly redesignated subsection 104(a)(6), 50 U.S.C. § 1804(a)(6), to require that an application for a court order under section 104 of FISA, 50 U.S.C. § 1804, include "a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official designated by the President to authorize electronic surveillance for foreign intelligence purposes".[14]

---

[13] Under current law, Section 104 of FISA, 50 U.S.C. § 1804, requires the federal officer seeking an order approving electronic surveillance under this section to make an application to a FISC judge in writing under oath or affirmation. The application must be approved by the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in FISA. Current subsections 104(a)(6), (9), and (11) of FISA, 50 U.S.C. §§ 1804(a)(6), (9), and (11), respectively, require that the application include:

> (6) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
>
> (9) a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application;
>
> (11) whenever more than one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device.

[14] Before amendment by Sec. 4(1)(C) of H.R. 5825, current subsection 104(a)(7) of FISA, 50 U.S.C. § 1804(a)(7) (redesignated 104(a)(6) of FISA, 50 U.S.C. § 1804(a)(6), by Sec. 4(1)(B) of H.R. 5825) requires that an application for a court order for electronic surveillance under section 104 of FISA, 50 U.S.C.§ 1804, is to include:

> (7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate —
>
> (A) that the certifying official deems the information sought to be foreign

(continued...)

- under Sec. 4(1)(C)(ii) of the bill, amend redesignated subsection 104(a)(6)(C) of FISA, new 50 U.S.C. § 1804(a)(6)(C) (previously subsection 104(a)(7)(C) of FISA, current 50 U.S.C. § 1804(a)(7)(C)), to add "and" at the end of it.

- under Sec. 4(1)(C)(iii) of the bill, strike redesignated subsections 104(a)(6)(D) and (E) of FISA, new 50 U.S.C. §§ 1804(a)(6)(D) and (E) (previously subsections 104(a)(7)(D) and (E) of FISA, current 50 U.S.C. §§ 1804(a)(7)(D) and (E)), and replace them with a new subsection 104(a)(6)(D) of FISA, new 50 U.S.C. § 1804(a)(6)(D), which would require the certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official designated by the President to authorize electronic surveillance for foreign intelligence purposes to include "a statement of the basis for the certification that the information sought is the type of foreign intelligence information designated."[15]

- under Sec. 4(1)(D) of the bill, amend redesignated subsection 104(a)(7) of FISA, new 50 U.S.C. § 1804(a)(7) (previously subsection 104(a)(8), current 50 U.S.C. § 1804(a)(8)), to read "a

---

[14] (...continued)

> intelligence information;
> (B) that a significant purpose of the surveillance is to obtain foreign intelligence information;
> (C) that such information cannot reasonably be obtained by normal investigative techniques;
> (D) that designates the type of foreign intelligence information being sought according to the categories described in section 101(e) [1801(e) of this title]; and
> (E) including a statement of the basis for the certification that —
> > (i) the information sought is the type of foreign intelligence information designated; and
> > (ii) such information cannot reasonably be obtained by normal investigative techniques[.]

[15] As so amended, newly redesignated subsection 104(a)(6) of FISA, 50 U.S.C. § 1804, would require an application for a court order authorizing electronic surveillance under section 104 of FISA, 50 U.S.C. § 1804 to include:

> (6) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official designated by the President to authorize electronic surveillance for foreign intelligence purposes —
> > (A) that the certifying official deems the information sought to be foreign intelligence information;
> > (B) that a significant purpose of the surveillance is to obtain foreign intelligence information;
> > (C) that such information cannot reasonably be obtained by normal investigative techniques; and
> > (D) including a statement of the basis for the certification that the information sought is the type of foreign intelligence information designated[.]

statement whether physical entry is required to effect the surveillance; and". Prior to this amendment, this subsection also required "a statement of the means by which the surveillance will be effected".

- under Sec. 4(1)(E) of the bill, amend redesignated subsection 104(a)(8) of FISA, new 50 U.S.C. § 1804(a)(8) (previously subsection 104(a)(10), current 50 U.S.C. § 1804(a)(10)), to replace the "; and" at the end of the subsection with "."

- under Sec. 4(2) of the bill, strike subsection 104(b) of FISA, 50 U.S.C. § 1804(b) (dealing with exclusion of certain informational requirements from applications for FISC orders authorizing electronic surveillance of certain types of foreign powers), and, under Sec. 4(3) of the bill, redesignate subsections 104(c), (d), and (e) of FISA, 50 U.S.C. §§ 1804(c), (d), and(e), as subsections 104(b), (c), and (d), new 50 U.S.C. §§ 1804(b), (c), and (d), respectively.[16]

---

[16] Current subsections 104(b), (c), (d), and (e) of FISA, 50 U.S.C. Secs. 1804(b), (c), (d), and (e), provide:

(b) Exclusion of certain information respecting foreign power targets

Whenever the target of the electronic surveillance is a foreign power, as defined in section 101 (a)(1), (2), or (3) [1801(a)(1), (2), or (3) of this title], and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the application need not contain the information required by paragraphs (6), (7)(E), (8), and (11) of subsection (a) of this section, but shall state whether physical entry is required to effect the surveillance and shall contain such information about the surveillance techniques and communications or other information concerning United States persons likely to be obtained as may be necessary to assess the proposed minimization procedures.

(c) Additional affidavits or certifications

The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

(d) Additional information

The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 105 [1805 of this title].

(e) Personal review by Attorney General

(1) (A) Upon written request of the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, or the Director of National Intelligence, the Attorney General shall personally review under subsection (a) of this section an application under that subsection for a target described in section 102(b)(2) [1801(b)(2) of this title].

(B) Except when disabled or otherwise unavailable to make a request referred to in subparagraph (A), an official referred to in that subparagraph

(continued...)

Sec. 5. Issuance of an Order

Sec. 5 amends section 105 of FISA, 50 U.S.C. § 1805, dealing with the requirements for issuance of an FISC order for electronic surveillance.

Sec. 5(1) addresses provisions which deal with the necessary findings that a FISC judge must make in issuing an ex parte order approving an application for a court order authorizing electronic surveillance under Sec. 105 of FISA, 50 U.S.C. § 1805. Sec. 5(1)(A) of the bill would strike subsection 105(a)(1) of FISA, 50 U.S.C. § 1805(a)(1).[17] Under Sec. 5(1)(B) of the bill, subsections 105(a)(2)-(5) of FISA

---

[16] (...continued)

> may not delegate the authority to make a request referred to in that subparagraph.
> (C) Each official referred to in subparagraph (A) with authority to make a request under that subparagraph shall take appropriate actions in advance to ensure that delegation of such authority is clearly established in the event such official is disabled or otherwise unavailable to make such request.
>
> (2) (A) If as a result of a request under paragraph (1) the Attorney General determines not to approve an application under the second sentence of subsection (a) of this section for purposes of making the application under this section, the Attorney General shall provide written notice of the determination to the official making the request for the review of the application under that paragraph. Except when disabled or otherwise unavailable to make a determination under the preceding sentence, the Attorney General may not delegate the responsibility to make a determination under that sentence. The Attorney General shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event the Attorney General is disabled or otherwise unavailable to make such determination.
> (B) Notice with respect to an application under subparagraph (A) shall set forth the modifications, if any, of the application that are necessary in order for the Attorney General to approve the application under the second sentence of subsection (a) of this section for purposes of making the application under this section.
> (C) Upon review of any modifications of an application set forth under subparagraph (B), the official notified of the modifications under this paragraph shall modify the application if such official determines that such modification is warranted. Such official shall supervise the making of any modification under this subparagraph. Except when disabled or otherwise unavailable to supervise the making of any modification under the preceding sentence, such official may not delegate the responsibility to supervise the making of any modification under that preceding sentence. Each such official shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event such official is disabled or otherwise unavailable to supervise the making of such modification.

[17] Current section 105(a) of FISA, 50 U.S.C. § 1805(a), deals with the necessary findings that a FISC judge must make in an ex parte order approving an application under section 104 of FISA, 50 U.S.C. § 1804, authorizing electronic surveillance. Under current section

(continued...)

would be redesignated subsections 105(a)(1)-(4) of FISA, 50 U.S.C. Secs. 1805(a)(1)-(4), respectively.

Subsection 105(c)(1) of FISA, 50 U.S.C. § 1805(c)(1), requires that an order approving electronic surveillance under Section 105 of FISA, 50 U.S.C. § 1805, must include certain specifications and sets out those specifications.[18] Sec. 5(2) of the bill would amend subsection 105(c)(1) of FISA, 50 U.S.C. § 1805(c)(1) to add "and" at the end of subparagraph 105(c)(1)(B) of FISA, 50 U.S.C. § 1805(c)(1)(B); delete subparagraphs 105(c)(1)(C), (D) and (F) of FISA, 50 U.S.C. §§ 1805(c)(1)(C), (D), and (F), and redesignate subparagraph 105(c)(1)(E) of FISA, 50 U.S.C. § 1805(c)(1)(E), as subparagraph 105(c)(1)(C), new 50 U.S.C. § 1805(c)(1)(C).

---

[17] (...continued)
105(a)(1) of FISA, 50 U.S.C. § 1805(a)(1), the FISC judge must find, in part, that "the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information."

[18] Current section 105(c)(1) of FISA, 50 U.S.C. § 1805(c)(1), provides:

> (c) Specifications and directions of orders
>
> (1) Specifications
> An order approving an electronic surveillance under this section shall specify —
> (A) the identity, if known, or a description of the specific target of the electronic surveillance identified or described in the application pursuant to section 104(a)(3) [1804(a)(3) of this title];
> (B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known;
> (C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;
> (D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance;
> (E) the period of time during which the electronic surveillance is approved; and
> (F) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the devices involved and what minimization procedures shall apply to information subject to acquisition by each device.

As amended, subsection 105(c)(1) would provide:

> (c) Specifications and directions of orders
>
> (1) Specifications
> An order approving an electronic surveillance under this section shall specify —
> (A) the identity, if known, or a description of the specific target of the electronic surveillance identified or described in the application pursuant to section 104(a)(3) [1804(a)(3) of this title];
> (B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known; and
> (C) the period of time during which the electronic surveillance is approved.

Current subsection 105(d) of FISA, 50 U.S.C. § 1805(d), deals with exclusion of certain information respecting foreign power targets from the ex parte order authorizing electronic surveillance under this section.[19] Sec. 5(3) of the bill strikes subsection 105(d) of FISA, 50 U.S.C. § 1805(d); and, under Sec. 5(4) of the bill, redesignates subsections 105(e)-(i) of FISA, 50 U.S.C. §§ 1805(e)-(i), as subsections 105(d)-(h) of FISA, 50 U.S.C. §§ 1805(d)-(h).

Under Sec. 5(5)(A) of the bill, pursuant to new subsection 105(d)(1) of FISA, new 50 U.S.C. § 1805(d)(1), an order under this section may approve electronic surveillance for up to one year.[20]

Under Sec. 5(5)(B) of the bill, new subsection 105(d)(2) of FISA, new 50 U.S.C. § 1805(d)(2), provides that extensions of orders for electronic surveillance under Section 105 may be granted for up to one year upon an application for an

---

[19] Current section 105(d) of FISA, 50 U.S.C. § 1805(d), provides:

> (d) Exclusion of certain information respecting foreign power targets
>
> Whenever the target of the electronic surveillance is a foreign power, as defined in section 101(a)(1), (2), or (3) [1801(a)(1), (2), or (3) of this title], and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the order need not contain the information required by subparagraphs (C), (D), and (F) of subsection (c)(1) of this section, but shall generally describe the information sought, the communications or activities to be subjected to the surveillance, and the type of electronic surveillance involved, including whether physical entry is required.

Subsections 101(a)(1), (2), or (3) of FISA, 50 U.S.C. §§ 1801(a)(1), (2), or (3) define "foreign power" to mean a foreign government or any component thereof, whether or not recognized by the United States; a faction of a foreign nation or nations, not substantially composed of United States persons; or an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments, respectively. Subparagraphs 105(c)(1)(C), (D), and (F) 50 U.S.C. §§ 1805(c)(1)(C), (D), and (F), are deleted by Sec. 5(2)(B) of the bill.

[20] Current section 105(e)(1) of FISA, 50 U.S.C. § 1805(e)(1) (which is redesignated section 105(d)(1) of FISA, 50 U.S.C. § 1805(d)(1) by H.R. 5825, Sec. 5(5)(A)), provides:

> (e) Duration of order; extensions; review of circumstances under which information was acquired, retained or disseminated
>
> (1) An order issued under this section may approve an electronic surveillance for the period specified in the application or for ninety days, whichever is less, except that (A) an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 101(a)(1), (2), or (3) [1801(a)(1), (2), or (3) of this title], for the period specified in the application or for one year, whichever is less, and (B) an order under this chapter for a surveillance targeted against an agent of a foreign power who is not a United States person may be for the period specified in the application or for 120 days, whichever is less.

extension and new findings made in the same manner as required for the original order.[21]

Under Sec. 5(6) of the bill, redesignated subsection 105(e) of FISA, new 50 U.S.C. § 1805(e) (under current law, subsection 105(f) of FISA, 50 U.S.C. § 1805(f)), provides authority for the Attorney General to authorize emergency employment of electronic surveillance if specific requirements are met. Under these requirements, the Attorney General must (1) determine 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) determine that the factual basis for issuance of an order under this title to approve such surveillance exists; (3) inform a FISC judge at the time of such authorization that the decision has been made to employ emergency electronic surveillance; and (4) make an application in accordance with this title to a FISC judge, as soon as practicable, but not more than 120 hours after the official authorizes such surveillance. Under current subsection 105(f) of FISA, 50 U.S.C. § 1805(f), the Attorney General's determinations in (1) and (2) above must be "reasonable," and an application for a FISC order authorizing the electronic surveillance must be made within 72 hours after the emergency electronic surveillance is authorized, rather than 120 hours as provided in the amended section under Sec. 5(6) of the bill. Sec. 5(6) also makes some non-substantive structural changes to the section.

Under the amendments in Sec. 5(6) of the bill to redesignated subsection 105(e) of FISA, 50 U.S.C. § 1805(e), if the Attorney General authorizes such emergency employment of electronic surveillance, he must 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 120 hours from the time of authorization by the Attorney General, whichever is earliest. If 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

---

[21] Current section 105(e)(2) of FISA, 50 U.S.C. § 1805(e)(2) (which is redesignated section 105(d)(2) of FISA, 50 U.S.C. § 1805(d)(2) by Sec. 5(5)(B) of H.R. 5825), reads:

> (2) Extensions of an order issued under this subchapter 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, except that (A) an extension of an order under this chapter for a surveillance targeted against a foreign power, as defined in section 101(a)(5) or (6) [1801(a)(5) or (6) of this title], or against a foreign power as defined in section 101(a)(4) [1801(a)(4) of this title] that is not a United States person, may be for a period not to exceed one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period, and (B) an extension of an order under this chapter for a surveillance targeted against an agent of a foreign power who is not a United States person may be for a period not to exceed 1 year.

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 indicates a threat of death or serious bodily harm to any person. A denial of the application made under this subsection may be reviewed as provided in section 103 of FISA, 50 U.S.C. § 1803. Under current law, in the absence of a court order approving the electronic surveillance, the surveillance must terminate when the information sought is obtained, when the application for an order is denied, or after the expiration of 72 hours from the time of authorization by the Attorney General, whichever is earlier. The provisions dealing with review of a denial of an application under this subsection and with limitations on use of the information gathered in an emergency electronic surveillance, where the application is denied or the surveillance is terminated and no court order approving the surveillance is issued, parallel those in current law.

Sec. 5(7) of the bill amends redesignated subsection 105(h) of FISA, new 50 U.S.C. § 1805(h) (current subsection 105(i) of FISA, 50 U.S.C. § 1805(i)), to bar court action in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance (1) in accordance with a court order or request for emergency assistance under this Act for electronic surveillance or physical search; or (2) 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 that does not constitute electronic surveillance. Clause (2) above adds new language to the existing provision. Thus, under current subsection 105(i), 50 U.S.C. § 1805(i), no such cause of action lies against those who furnish information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under FISA for electronic surveillance or physical search. There is no parallel bar in current law to court action against those providing such information, facilities, or technical assistance in response to a certification by the Attorney General or his designee seeking information, facilities, or technical assistance from such person that does not constitute electronic surveillance.

Sec. 6. Use of Information

Sec. 6 of H.R. 5825 amends subsection 106 of FISA, 50 U.S.C. § 1806, dealing with use of information obtained by or derived from electronic surveillance under title I of FISA. As amended, subsection 106(i) of FISA would provide for destruction upon recognition of the contents of any communication unintentionally acquired by an electronic, mechanical, or other surveillance device, under circumstances in which a person has a reasonable expectation of privacy, a warrant would be required for law enforcement purposes, and both the sender and all intended recipients are located within the United States, unless the Attorney General

determines that the contents contain significant foreign intelligence information or indicate a threat of death or serious bodily harm to any person.

Sec. 7. Authorization after an Armed Attack

Sec. 7(a) amends section 111 of FISA, 50 U.S.C. § 1811, to authorize electronic surveillance to acquire foreign intelligence information without a court order for up to 60 days following an armed attack against the territory of the United States if the President submits to each member of the congressional intelligence "committee" [It seems likely that this should be "committees".] notification of the authorization under this section. Current law authorizes electronic surveillance without a FISA court order to acquire foreign intelligence information for up to 15 calendar days after a declaration of war by Congress.

Sec. 7(b) of the bill amends section 309 of FISA, 50 U.S.C. § 1829, to authorize physical searches to acquire foreign intelligence information without a court order for up to 60 days following an armed attach against the territory of the United States if the President submits to each member of the congressional intelligence "committee" [Again, it seems likely that this should be "committees".] notification of the authorization under this section. Current law authorizes physical searches without a FISA court order to acquire foreign intelligence information for up to 15 calendar days after a declaration of war by Congress.

Sec. 8. Authorization of Electronic Surveillance after a Terrorist Attack

Sec. 8(1) of the bill creates a new section 112 of FISA entitled "Authorization Following A Terrorist Attack Upon the United States." New subsection 112 (a) permits the President, acting through the Attorney General, to authorize electronic surveillance without a FISA order approving such surveillance, for a period not to exceed 45 days following a terrorist attack against the United States if the President submits a notification to each member of the congressional intelligence committees and a FISC judge that (1) the United States has been the subject of a terrorist attack; and (2) identifies the terrorist organizations or affiliates of terrorist organizations believed to be responsible for the terrorist attack.

Under Sec. 8(1) of the bill, new subsection 112(b) of FISA provides that, subject to subsection 112(d) (which prohibits the President from authorizing electronic surveillance under section 112 until the Attorney General approves applicable minimization procedures), at the end of the 45 day period described in new subsection 112(a) of FISA, and every 45 days thereafter, the President may submit a subsequent notification to the congressional intelligence committees and to a FISC judge that the circumstances of the terrorist attack for which the President submitted a subsection 112(a) certification "require the President to continue the authorization of electronic surveillance under this section for an additional 45 days." After each subsequent certification, the President "shall be authorized to conduct electronic surveillance under this section for an additional 45 days."

Sec. 8(1) of the bill creates a new subsection 112(c) of FISA dealing with electronic surveillance of individuals. Under this new subsection, the President, or an official designated by the President to authorize electronic surveillance, may only conduct electronic surveillance of a person under this subsection when the President or such official determines that (1) there is a reasonable belief that such person is communicating with a terrorist organization or an affiliate of a terrorist organization that is reasonably believed to be responsible for the terrorist attack; and (2) the information obtained from the electronic surveillance may be foreign intelligence information.

Under new subsection 112(d) of FISA, as created by Sec. 8(1) of H.R. 5825, the President may not authorize electronic surveillance under section 112 until the Attorney General approves applicable minimization procedures.

New subsection 112(e) of FISA, as created by Sec. 8(1) of the bill, addresses electronic surveillance of U.S. persons. It provides that, notwithstanding new subsection 112(b) of FISA, the President may not authorize electronic surveillance of a United States person under section 112 of FISA without a FISC order for a period of more than 90 days unless the President, acting through the Attorney General, submits a certification to each member of the congressional intelligence committees that "(1) the continued electronic surveillance of the United States person is vital to the national security of the United States; (2) describes the circumstances that have prevented the Attorney General from obtaining an order under this title for continued surveillance; (3) describes the reasons for believing the United States person is affiliated with or in communication with a terrorist organization or affiliate of a terrorist organization that is reasonably believed to be responsible for the terrorist attack; and (4) describes the foreign intelligence information derived from the electronic surveillance conducted under this section."

Under Sec. 8(1) of the bill, new subsection 112(f) of FISA permits information obtained pursuant to electronic surveillance under subsection 112 to be used to obtain an order authorizing subsequent electronic surveillance under FISA.

New subsection 112(g), as added by Sec. 8(1) of the bill, provides that, not later than 14 days after the date on which the President notifies each member of the congressional intelligence committees and a FISC judge of his intent to permit electronic surveillance without a FISA order for 45 days following a terrorist attack against the United States (under subsection 112(a)), and every 30 days thereafter until such surveillance ceases to be authorized by the President, the President must submit to each member of the congressional intelligence committees a report on the electronic surveillance conducted under section 112, including (1) a description of each target of electronic surveillance under this section; and (2) the basis for believing that each target is in communication with a terrorist organization or an affiliate of a terrorist organization.

New subsection 112(h) of FISA, added by Sec. 8(1) of H.R. 5825, defines the term "congressional intelligence committees" to mean the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate.

Sec. 8(2) of the bill adds new section 112 to the table of contents of FISA.

Sec. 9. Congressional Oversight

Sec. 9 of H.R. 5825 deals with congressional oversight. Sec. 9(a)(1) of the bill amends section 108(a)(1) of FISA, 50 U.S.C. § 1808(a)(1), to require that the Attorney General, on a semiannual basis, fully inform *each member* of the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, and the Committee on the Judiciary of the Senate, concerning all foreign intelligence electronic surveillance. (Italics reflect new language.) Sec. 9(a)(2) of the bill adds a new subsection 108(a)(2)(D) of FISA, 50 U.S.C. § 1808(a)(2)(D) which requires that each of these semiannual reports include a description of "the authority under which the electronic surveillance is conducted." Sec. 9(a)(3) of H.R. 5825 adds a new subsection (3) to the end of subsection 108(a) of FISA, 50 U.S.C. § 1808(a)(3), which requires each report submitted under this subsection 108(a) of FISA, 50 U.S.C. § 1808(a) to include "reports on electronic surveillance conducted without a court order."[22]

---

[22] Current section 108(a) of FISA, 50 U.S.C. § 1808(a), provides:

> § 1808. Report of Attorney General to Congressional committees; limitation on authority or responsibility of information gathering activities of Congressional committees; report of Congressional committees to Congress
>
> (a) (1) On a semiannual basis the Attorney General shall fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, and the Committee on the Judiciary of the Senate, concerning all electronic surveillance under this subchapter. Nothing in this subchapter shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties.
> (2) Each report under the first sentence of paragraph (1) shall include a description of —
> (A) the total number of applications made for orders and extensions of orders approving electronic surveillance under this subchapter where the nature and location of each facility or place at which the electronic surveillance will be directed is unknown;
> (B) each criminal case in which information acquired under this chapter has been authorized for use at trial during the period covered by such report; and
> (C) the total number of emergency employments of electronic surveillance under section 105(f) [1805(f) of this title] and the total number of subsequent orders approving or denying such electronic surveillance.

As amended by Sec. 10(4) of H.R. 5825, the reference to section 105(f), 50 U.S.C. § 1805(f), would be replaced by a reference to new section 105(e), new 50 U.S.C. § 1805(e), to be consistent with changes in Sec. 5(4) of the bill.

Sec. 9(b) of H.R. 5825 amends Section 501 of the National Security Act of 1947, 50 U.S.C. § 413,[23] to require, under subsection 501(a)(1) of the National Security Act, 50 U.S.C. § 413(a)(1), that the President shall ensure that *each member* of the congressional intelligence committees is kept fully and currently informed of the intelligence activities of the United States; and, under section 501(b) of the National Security Act, 50 U.S.C. § 413(b), that the President shall ensure that any illegal intelligence activity is reported promptly to *each member* of the congressional intelligence committees, as well as any corrective action that has been taken or is planned in connection with such illegal activity. (Italics reflect new language.)

---

[23] Current section 501 of the National Security Act of 1947, 50 U.S.C. § 413, provides:

§ 413. General Congressional oversight provisions

(a) Reports to Congressional committees of intelligence activities and anticipated activities

(1) The President shall ensure that the congressional intelligence committees are kept fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity as required by this subchapter.

(2) Nothing in this subchapter shall be construed as requiring the approval of the congressional intelligence committees as a condition precedent to the initiation of any significant anticipated intelligence activity.

(b) Reports concerning illegal intelligence activities

The President shall ensure that any illegal intelligence activity is reported promptly to the congressional intelligence committees, as well as any corrective action that has been taken or is planned in connection with such illegal activity.

(c) Procedures for reporting information

The President and the congressional intelligence committees shall each establish such procedures as may be necessary to carry out the provisions of this subchapter.

(d) Procedures to protect from unauthorized disclosure

The House of Representatives and the Senate shall each establish, by rule or resolution of such House, procedures to protect from unauthorized disclosure all classified information, and all information relating to intelligence sources and methods, that is furnished to the intelligence committees or to Members of Congress under this subchapter. Such procedures shall be established in consultation with the Director of National Intelligence. In accordance with such procedures, each of the congressional intelligence committees shall promptly call to the attention of its respective House, or to any appropriate committee or committees of its respective House, any matter relating to intelligence activities requiring the attention of such House or such committee or committees.

(e) Construction of authority conferred

Nothing in this Act shall be construed as authority to withhold information from the congressional intelligence committees on the grounds that providing the information to the intelligence committees would constitute the unauthorized disclosure of classified information or information relating to intelligence sources and methods.

(f) "Intelligence activities" defined

As used in this section, the term "intelligence activities" includes covert actions as defined in section 413b(e) of this title, and includes financial intelligence activities.

Sec. 10. Technical and Conforming Amendments

Sec. 10 of H.R. 5825 makes technical and conforming amendments to FISA. Under Sec. 10(1) of the bill, subsection 102(a)(3)(A) of FISA, 50 U.S.C. § 1802(a)(3)(A), would be amended to strike "101(h)(4) and". As amended by H.R. 5825, subsection 102(a)(3) of FISA, 50 U.S.C. § 1802(a)(3), would then read,

> (3) The Attorney General shall immediately transmit under seal to the court established under section 103(a) [1803(a) of this title] a copy of his certification. 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 —
>
> (A) an application for a court order with respect to the surveillance is made under sections [sic?] 104 [1804 of this title]; or
>
> (B) the certification is necessary to determine the legality of the surveillance under section 106(f) [1806(f) of this title].

Sec. 10(2) of H.R. 5825 would amend section 105(a)(5) of FISA, 50 U.S.C. § 1805(a)(5), by replacing "104(a)(7)(E)" with "104(a)(6)(D)", and replacing "104(d)" with "104(c)". Section 105(a)(5) of FISA, 50 U.S.C. § 1805(a)(5), would then read:

> (a) Necessary findings
> Upon an application made pursuant to section 104 [1804 of this title], the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that —
> . . .
> (5) the application which has been filed contains all statements and certifications required by section 104 [1804 of this title] and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 104(a)(6)(D) [1804(a)(6)(D) of this title] and any other information furnished under section 104(c) [1804(c) of this title].

This change would conform with amendments made in Secs. 4(1)(B), 4(1)(C)(ii) and 4(1)(C)(iii) of H.R. 5825.

Sec. 10(3)(A) of H.R. 5825 would amend subsection 106(j) of FISA, 50 U.S.C. § 1806(j) by replacing "105(e)" in the matter preceding paragraph 106(j)(1) with "105(d)". As amended by Sec. 10(3)(A) of H.R. 5825, the introductory language prior to subsection 106(j)(1) of FISA, 50 U.S.C. § 1806(j)(1), would then read,

> (j) Notification of emergency employment of electronic surveillance; contents; postponement, suspension or elimination
> If an emergency employment of electronic surveillance is authorized under section 105(d) [1805(d) of this title] and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of —
> . . . .

The change would conform with amendments in Secs. 5(3) and 5(4) of the bill.

In subsection 106(k)(2) of FISA, 50 U.S.C. § 1806(k)(2), Sec. 10(3)(B) of H.R. 5825 would replace "104(a)(7)(B)" with "104(a)(6)(B)". As amended by Sec. 10(3)(B) of the bill, subsection 106(k)(2) of FISA, 50 U.S.C. § 1806(k)(2) would then provide, "(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 104(a)(6)(B) [1804(a)(7)(B) of this title] or the entry of an order under section 105 [1805 of this title]." This change would conform with the amendments made in Secs. 4(1)(B), 4(1)(C)(ii) and 4(1)(C)(iii) of H.R. 5825.

Sec. 10(4) of H.R. 5825 would amend subsection 108(a)(2)(C) of FISA, 50 U.S.C. § 1808(a)(2)(C) to strike "105(f)" and insert in its stead "105(e)". In so doing, the reference is made consistent with the redesignation, in Sec. 5(4) of H.R. 5825, of current subsection 105(f) of FISA, 50 U.S.C. § 1805(f), as subsection 105(e) of FISA, new 50 U.S.C. § 1805(e).

crsphpgw

GalleryWatch
http://www.crsdocuments.com
Penny Hill Press