Order Code RL34143

CRS Report for Congress

P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act

Updated February 14, 2008

Elizabeth B. Bazan
Legislative Attorney
American Law Division

Prepared for Members and Committees of Congress

P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act

Summary

On August 5, 2007, P.L. 110-55, the Protect America Act of 2007, was signed into law by President Bush, after having been passed by the Senate on August 3 and the House of Representatives on August 4. The measure, introduced by Senator McConnell as S. 1927 on August 1, makes a number of additions and modifications to the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, 50 U.S.C. §§ 1801 *et seq*., and adds additional reporting requirements. As originally passed, the law was to sunset in 180 days, on February 1, 2008. On January 29, 2008, both the House and the Senate passed H.R. 5104, a 15-day extension to the sunset for the Protect America Act, to allow further time to consider, pass, and go to conference on proposed legislation to amend FISA, while ensuring that the intelligence community would have the authority it needed in the intervening period. Signed into law on January 31, it became P.L. 110-182. On February 13, 2008, the House rejected H.R. 5349, which would have extended the sunset provision an additional 21 days. Bills have been introduced in the Senate to extend the sunset from 180 to 210 days (S. 2541, S. 2556, and S. 2615) or to extend it to July 1, 2009 (S. 2557).

The Foreign Intelligence Surveillance Act of 1978 was enacted in response both to the Committee to Study Government Operations with Respect to Intelligence Activities (Church Committee) revelations with regard to past abuses of electronic surveillance for national security purposes and to the somewhat uncertain state of the law on the subject. In creating a statutory framework for the use of electronic surveillance to obtain foreign intelligence information, the Congress sought to strike a balance between national security interests and civil liberties. Critical to an understanding of the FISA structure are its definitions of terms such as "electronic surveillance" and "foreign intelligence information." P.L. 110-55 limits the construction of the term "electronic surveillance" so that it does not cover surveillance directed at a person reasonably believed to be located outside the United States. It also creates a mechanism for acquisition, without a court order under a certification by the Director of National Intelligence (DNI) and the Attorney General, of foreign intelligence information concerning a person reasonably believed to be outside the United States. The Protect America Act provides for review by the Foreign Intelligence Surveillance Court (FISC) of the procedures by which the DNI and the Attorney General determine that such acquisitions do not constitute electronic surveillance. In addition, P.L. 110-55 authorizes the Attorney General and the DNI to direct a person with access to the communications involved to furnish aid to the government to facilitate such acquisitions, and provides a means by which the legality of such a directive may be reviewed by the FISC petition review pool. A decision by a judge of the FISC petition review pool may be appealed to the Foreign Intelligence Surveillance Court of Review, and review by the U.S. Supreme Court may be sought by petition for writ of certiorari. This report describes the provisions of P.L. 110-55, discusses its possible impact on and parallels to existing law, summarizes the legislative activity with respect to S. 1927, H.R. 3356, and S. 2011, and touches on recent legislative developments. It will be updated as needed.

Contents

P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act

Introduction

In response to concerns raised by the Director of National Intelligence, Admiral Mike McConnell, that the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801 *et seq*., required modernization to meet the current intelligence needs of the nation, a number of bills were introduced in the Senate and the House of Representatives. Intense legislative activity with respect to proposed amendments to FISA in both bodies resulted in the enactment of the Protect America Act of 2007, P.L. 110-55 on August 5, 2007. The measure was introduced as S. 1927 by Senator McConnell, for himself and Senator Bond, on August 1, 2007. The bill was considered in the Senate on August 3, in conjunction with S. 2011, entitled The Protect America Act of 2007, introduced by Senator Levin, for himself and Senator Rockefeller. The Senate agreed by unanimous consent to an amendment to S. 1927 offered by Senator McConnell, for himself and Senator Bond, providing that sections 2, 3, 4, and 5 of the bill would sunset 180 days after its enactment.[1] As amended, S. 1927 passed the Senate the same day.[2] S. 2011 did not receive the requisite 60 votes, and was placed on the Senate calendar under general orders.[3]

That evening, the House considered H.R. 3356, the Improving Foreign Intelligence Surveillance to Defend the Nation and the Constitution Act of 2007, introduced by Representative Reyes for himself, Representative Conyers, Representative Schiff, and Representative Flake. After a motion to suspend the rules and pass H.R. 3356 fell short of the required two-thirds vote of the Members[4] on Friday night, the House took up S. 1927 the following day. At 10:19 p.m. Saturday night, August 4, the House passed S. 1927.[5] It was signed by the President on August 5, 2007. On January 29, 2008, both the House and the Senate passed H.R. 5104, a 15-day extension to the sunset for the Protect America Act, to allow further time to consider, pass, and go to conference on proposed legislation to amend FISA, while ensuring that the intelligence community would have the authority it needed in the intervening period. The President signed the measure into law on January 31, 2008,

---

[1] S.Amdt. 2649 to S. 1927.

[2] Record Vote Number 309, 60-28 (August 3, 2007).

[3] Record Vote Number 310, 43-45 (August 3, 2007).

[4] The August 3, 2007, vote on the motion to suspend the rules and pass H.R. 3356 was 218 - 207 (Roll no. 821).

[5] The bill was passed by the Yeas and Nays: 227 - 183 (Roll no. 836).

as P.L. 110-182. On February 13, 2008, the House rejected H.R. 5349, which would have extended the sunset provision for an additional 21 days. Bills have been introduced in the Senate to extend the sunset from 180 to 210 days (S. 2541, S. 2556, and S. 2615), or to extend it to July 1, 2009 (S. 2557).

This report discusses the provisions of P.L. 110-55 and their impact on or relationship with the prior provisions of FISA.

Sec. 1. Short Title

Sec. 1 of S. 1927 states that the short title of the law is the Protect America Act of 2007.

Sec. 2. Additional Procedures for Authorizing Certain Acquisitions of Foreign Intelligence Information

Section 2 of the law contains its first substantive provisions. They are summarized in order below.

New Section 105A of FISA, "Clarification of Electronic Surveillance of Persons Outside the United States"

New Section 105A of FISA, as added by Section 2 of P.L. 110-55, states:

> Nothing in the definition of electronic surveillance under section 101(f) shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States.

Section 101(f) of FISA, 50 U.S.C. § 1801(f), sets forth the definition of "electronic surveillance" under the statute. It provides:

> (f) "Electronic surveillance" means —
>
> (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[6] who is in the United

---

[6] As defined in section 101(i) of FISA, 50 U.S.C. § 1801(i),

> "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), 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

(continued...)

> 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.

To what extent would the new section 105A affect the scope of "electronic surveillance" as defined in section 101(f) of FISA? Absent the interpretation required by section 105A, two of the four definitions of "electronic surveillance" under section 101(f) of FISA, by their terms, appear to be broad enough to encompass electronic surveillance directed at a person abroad where the communications involved transcend U.S. borders.[7] Subsections 101(f)(2) and (f)(4) of FISA, on their face, appear to have the potential of reaching electronic surveillance of such communications targeted at a person outside the United States. In addition, it might be argued that the language of subsection 101(f)(4) might encompass the possibility of reaching some foreign to foreign communications in limited

---

[6] (...continued)
(a)(1), (2), or (3) of this section.

"Foreign power," as defined in section 101(a)(1), (2), or (3), 50 U.S.C. § 1801(a)(1), (2), or (3), means:

> (1) a foreign government or any component thereof, whether or not recognized by the United States;
> (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
> (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments[.]

[7] Because new section 105A of FISA explicitly addresses electronic surveillance "directed at a person reasonably believed to be located outside the United States," it would not appear to affect subsection 101(f)(1), which deals with electronic surveillance of the contents of wire or radio communications acquired from an *intentionally targeted U.S. person within the United States* under specified circumstances. "Electronic surveillance" as defined in subsection 101(f)(3) of FISA involves the intentional acquisition of the contents of radio communications in specified circumstances *where the sender and all the intended recipients to the communication are in the United States*, so it would not seem to be impacted by new section 105A.

circumstances. This would suggest that, under FISA prior to the passage of section 105A of P.L. 110-55, some interceptions directed at a person abroad covered by the language of these subsections might have been regarded by the FISC as requiring court authorization.[8]

In pertinent part, "electronic surveillance," as defined by subsection 101(f)(2), covers acquisition of the contents of wire communications to or from a person in the United States where the acquisition occurs within the United States and no party to the communication has consented to the interception. Unlike subsection 101(f)(1), there is no express requirement that the person in the United States be known, that he or she be United States person, or that he or she be intentionally targeted by the electronic surveillance.

To the extent that an electronic surveillance under subsection 101(f)(2) intercepts communications between persons in the United States, it would not be impacted by section 105A of FISA, as added by P.L. 110-55, nor would section 105A affect electronic surveillance targeted at a person within the United States. However, to the extent that the language in subsection 101(f)(2) might encompass interception of communications between a person in the United States and one or more parties outside the United States, where the surveillance is targeted at a person outside the United States, section 105A would seem to restrict the previous reach of the definition of "electronic surveillance" in section 101(f)(2).

Subsection 101(f)(4) defines "electronic surveillance" under FISA to include "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,[9] under circumstances in which a person has a reasonable

---

[8] *See,* Greg Miller, "The Nation: Spy chief sheds light on wiretaps; The intelligence director confirms that the FISA court ruled against Bush's surveillance program," *Los Angeles Times,* August 23, 2007, at A14, available at [http://pqasb.pqarchiver.com/latimes/access/1324701671.html?dids=1324701671:1324701671&FMT=ABS&FMTS=ABS:FT&type=current&date=Aug+23,+2007&author=Greg+Miller&pub=Los+Angeles+Times&edition=&startpage=A.14&desc=The+Nation;+Spy+chief+sheds+light+on+wiretaps;+The+intelligence+director+confirms+that+the+FISA+court+ruled+against+Bush's+surveillance+program].

[9] Section 101(l) of FISA, 50 U.S.C. § 1801(l), defines "wire communication" to mean:

> (l) "Wire communication" means 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.

It does not have a separate definition of "radio communication." However, subsection 101(f)(4) of FISA appears to contemplate that communications can be transmitted using technologies other wire or radio. For example, in Title III of the Omnibus Crime Control and Safe Streets Act, as amended, 18 U.S.C. § 2510(12), "electronic communication" includes other technologies. Under § 2510(12), this term is defined to mean:

(continued...)

expectation of privacy and a warrant would be required for law enforcement purposes." This subsection does not explicitly address the location of the parties to the communication or the location of the acquisition of the information involved. Thus, by its terms, it could conceivably be interpreted to cover some communications between parties in the United States, between a party in the United States and a party outside the United States, or between parties abroad, if the other requirements of the subsection were satisfied. The restrictions in this section are two-fold: the information must be acquired other than from a wire or radio communication; and the circumstances of the acquisition must be such that a person would have a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. To the extent that "electronic surveillance" under subsection 101(f)(4) of FISA could have been or has been directed at a person or persons abroad, prior to the enactment of P.L. 110-55, new section 105A may also have the effect of limiting the scope of this subsection of the definition of "electronic surveillance" as it was previously interpreted.

New Section 105B of FISA, "Additional Procedure for Authorizing Certain Acquisitions Concerning Persons Located Outside the United States"

New section 105B(a) of FISA permits the Attorney General and the Director of National Intelligence, for periods of up to one year, to authorize acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States, if the Attorney General and the DNI determine, based on the information provided to them, that five criteria have been met. Under these criteria, the Attorney General and the DNI must certify that:

> (1) there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States,[10] and such

---

[9] (...continued)

> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include —
>
> (A) any wire or oral communication;
> (B) any communication made through a tone-only paging device;
> (c) any communication from a tracking device (as defined in [18 U.S.C. § 3117]); or
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds[.]

[10] The reporting requirements in Sec. 4 of the P.L. 110-55 require, in part, that the Attorney General report to the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, and the House and Senate Judiciary Committees regarding incidents of non-compliance by an element of the Intelligence Community with guidelines or procedures for determining that the acquisition of foreign intelligence authorized by the DNI and the Attorney General under section 105B "concerns persons reasonably [sic?] to (continued...)

procedures will be subject to review of the Court pursuant to section 105C of this Act;[11]
(2) the acquisition does not constitute electronic surveillance;
(3) the acquisition involves obtaining the foreign intelligence information from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications;
(4) a significant purpose of the acquisition is to obtain foreign intelligence information; and
(5) the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h).[12]

---

[10] (...continued)
be outside the United States."

[11] Section 105B(a)(1) states that the "procedures for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States" are to be submitted to the FISC for review pursuant to section 105C of FISA. There appears to be some ambiguity in the language of section 105B, particularly as compared with section 105C, as to what the procedures cover and what procedures are to be submitted to the FISC. The phrasing of section 105B(a)(1) on its face, seems to require submission to the FISC only of "reasonable procedures . . . for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States." This is the only mention in section 105B of procedures being submitted to the FISC. Thus, there is no mention in section 105B of creation of, or submission to the FISC of, procedures upon which the government bases its determination that the acquisition does not constitute electronic surveillance.

However, section 105C, by its terms, addresses only the submission by the Attorney General to the FISC of the procedures by which the government determines that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance, making no mention of the procedures referred to in section 105B(a)(1). In light of this apparent inconsistency, it is unclear what review, if any, the FISC is intended to give the procedures for determining that the acquisition of foreign intelligence information under section 105B "concerns persons reasonably believed to be located outside the United States." It is also not made clear in the language of either section by whom the procedures to be reviewed by the FISC under section 105C are to be promulgated.

On the other hand, section 105A provides that the definition of "electronic surveillance" shall not be "construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States." In light of this, it might be argued that the procedures by which the DNI and the Attorney General determine whether an acquisition of foreign intelligence information under section 105B concerns persons reasonably believed to be located outside the United States could be regarded as part of the FISC's analysis as to whether the procedures to determine that the acquisitions under 105B constitute electronic surveillance are clearly erroneous.

[12] Section 101(h) of FISA, 50 U.S.C. § 1801(h), defines "minimization procedures" for purposes of title I of FISA, dealing with electronic surveillance, to mean:

(h) "Minimization procedures", with respect to electronic surveillance, means —
(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the

(continued...)

Except in circumstances where immediate government action is required and there is not sufficient time to prepare a certification, the determination by the Attorney General and the DNI that these criteria have been satisfied must be in the form of a certification, under oath, supported by affidavit of appropriate officials in the national security field appointed by the President, by and with the advice and consent of the Senate, or the Head of any agency of the Intelligence Community. Where imminent government action is required, the determination must be reduced to a certification as soon as possible within 72 hours after the determination is made.[13] The certification need not identify specific facilities, places, premises, or property at which the acquisition will be directed.[14]

---

[12] (...continued)

> particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
> (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
> (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
> (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, 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.

It may be noted that, while section 105B of FISA appears to be located in title I of FISA, which deals with electronic surveillance, the DNI and the Attorney General, under section 105B(a)(2) of FISA, are expressly required to certify that the acquisitions under section 105B do *not* constitute electronic surveillance. Similarly, the minimization procedures in section 101(h) of FISA, 50 U.S.C. § 1801(h), deal explicitly with minimization in the context of electronic surveillance, while, under subsection 105B(a)(5) of FISA, the DNI and the Attorney General must certify that "the minimization procedures to be used with respect to such acquisition[s] meet the definition of minimization procedures under section 101(h)." This seems likely to be intended to mean that the minimization procedures applicable to such acquisitions must set parallel standards to those applicable to electronic surveillance under the minimization procedures in section 101(h) of FISA, 50 U.S.C. § 1801(h).

[13] Protect America Act of 2007, P.L. 110-55, Sec. 105B(a), 121 Stat. 552 (August 5, 2007) (hereinafter P.L. 110-55).

[14] P.L. 110-55, Sec. 105B(b).

A copy of a certification made under section 105B(a) must be transmitted under seal to the FISC as soon as practicable, there to be maintained under security measures established by the Chief Justice of the United States and the Attorney General, in consultation with the DNI. The copy of the certification must remain sealed unless needed to determine the legality of the acquisition involved.[15]

Where a certification has been prepared, an acquisition under section 105B of FISA must be conducted in accordance with that certification and minimization procedures adopted by the Attorney General. If a certification has not yet been prepared because of inadequate time, the acquisition must comply with the oral instructions of the DNI and the Attorney General and the applicable minimization procedures.[16] Section 105B(d) requires the DNI and the Attorney General must report their assessments of compliance with "such procedures"[17] to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence under section 108(a) of FISA, 50 U.S.C. § 1808(a).[18]

---

[15] P.L. 110-55, Sec. 105B(c).

[16] P.L. 110-55, Sec. 105B(d).

[17] In the context of the subsection 105B(d), the reference to "such procedures" might be seen to be susceptible of two possible interpretations. Perhaps the more likely and more limited interpretation would be that this may be a reference to the applicable minimization procedures referenced earlier in the subsection. Alternatively, a more expansive view might interpret this as a reference to the applicable minimization procedures plus the relevant certification, including the "reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States," or oral instructions regarding the acquisition at issue.

[18] Section 108 of FISA, 50 U.S.C. § 1808, 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 [title I of FISA, 50 U.S.C. §§ 1801 *et seq*.]. Nothing in this subchapter [title I of FISA] 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
>
> (continued...)

In connection with an acquisition authorized under section 105B, the DNI and the Attorney General may issue a directive to a person to immediately provide the government with all information , facilities, and assistance needed to accomplish the acquisition in a manner which will protect the secrecy of the acquisition and minimize interference with the services provided by that person to the target of the acquisition.[19] The government must compensate the person furnishing such aid at the prevailing rate.[20] Any records that person wishes to keep relating to the acquisition or the aid provided must be maintained under security procedures approved by the DNI and the Attorney General.[21] P.L. 110-55 bars any cause of action in any court against any person for providing information, facilities or assistance in accordance with a directive under this section.[22] If a person receiving such a directive fails to comply therewith, the FISC, at the Attorney General's request, shall issue an order to compel such compliance if the court finds that the directive was issued in accordance with section 105B(e) and is otherwise lawful.[23]

---

[18] (...continued)

> by such report; and
> (C) the total number of emergency employments of electronic surveillance under section 1805(f) of this title and the total number of subsequent orders approving or denying such electronic surveillance.
>
> (b) On or before one year after October 25, 1978, and on the same day each year for four years thereafter, the Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence shall report respectively to the House of Representatives and the Senate, concerning the implementation of this chapter. Said reports shall include but not be limited to an analysis and recommendations concerning whether this chapter should be (1) amended, (2) repealed, or (3) permitted to continue in effect without amendment.

It may be noted that the reporting requirements under subsection 108(a) of FISA deal explicitly with electronic surveillance under FISA, and impose responsibility only upon the Attorney General. While section 105B has been added to title I of FISA, which deals with electronic surveillance, the DNI and the Attorney General, under subsection 105B(a)(2) are required to certify, with respect to each acquisition under section 105B, that such acquisition "does not constitute electronic surveillance." The reporting requirement in section 105B(d) may be intended to direct the DNI and the Attorney General to include their assessments with respect to the procedures involved in the semiannual report of the Attorney General required by section 108(a), or it may be intended to require that the DNI and the Attorney General fully inform the House and Senate Intelligence Committees of their assessments on a semi-annual basis.

[19] P.L. 110-55, Sec. 105B(e)(1).

[20] P.L. 110-55, Sec. 105B(f).

[21] P.L. 110-55, Sec. 105B(e)(2).

[22] P.L. 110-55, Sec. 105B(l).

[23] P.L. 110-55, Sec. 105B(g). Service of process may be made upon such person in any judicial district in which he or she is found.

A person receiving a directive under section 105B(e) may challenge its legality by filing a petition before the petition review pool of the FISC.[24] Under subsection 105B(h)(1)(B) as written, the presiding judge of the Foreign Intelligence Surveillance Court of Review (Court of Review)[25] shall assign a petition filed with the petition review pool to one of the FISC judges in the pool. The assigned judge must conduct an initial review of the directive within 48 hours after the assignment. If he or she determines that the petition is frivolous, the petition is immediately denied and the directive or that portion of the directive that is the subject of the petition is affirmed.

---

[24] Section 103(e)(1) of FISA, 50 U.S.C. § 1803(e)(1), established this pool. As amended by Sec. 5 of P.L. 110-55, section 103(e) provides:

> (e) (1) Three judges designated under subsection (a) of this section who reside within 20 miles of the District of Columbia, or, if all of such judges are unavailable, other judges of the court established under subsection (a) of this section as may be designated by the presiding judge of such court, shall comprise a petition review pool which shall have jurisdiction to review petitions filed pursuant to section *105B(h) or 501(f)(1)* of [FISA].
> (2) Not later than 60 days after March 9, 2006, the court established under subsection (a) of this section shall adopt and, consistent with the protection of national security, publish procedures for the review of petitions filed pursuant to section *105B(h) or 501(f)(1)* of [FISA] by the panel established under paragraph (1). Such procedures shall provide that review of a petition shall be conducted in camera and shall also provide for the designation of an acting presiding judge. [Emphasis added.]

Subsection 103(a) requires the Chief Justice of the United States to publicly designate 11 U.S. district court judges from seven of the United States judicial circuits to become the FISC judges. The reference to section 501(f)(1) of FISA, 50 U.S.C. § 1861(f)(1), may be intended to be a reference to section 501(f), 50 U.S.C. § 1861(f). Section 501(f), as added to FISA by P.L. 109-177, § 106(f), was rewritten by P.L. 109-178, § 3. Current section 501(f)(1) of FISA contains two subsections, defining the terms "production order" and "nondisclosure order," respectively, for purposes of section 501.

[25] Section 105B(h)(1)(B) states that the "presiding judge designated pursuant to section 103(b) shall assign a petition filed under subparagraph (a) to one of the judge serving in the pool established by section 103(e)(1)." This may be intended to refer to the presiding judge of the FISC designated pursuant to section 103(a), rather than the presiding judge of the Foreign Intelligence Surveillance Court of Review designated pursuant to section 103(b). The petition review pool established by section 103(e)(1) is made up of FISC judges. *See* footnote 24, *supra*. Section 501(f)(2)(A)(ii) provides that, when a petition under that section is filed with the petition review pool of the FISC, "the presiding judge" shall immediately assign it to one of the judges in the pool. The rules, effective May 5, 2006, promulgated by the FISC under section 103(e)(2) of FISA are more explicit. Under title III, sections 8 and 9, of the "Procedures for review of Petitions filed pursuant to Section 501(f) of the Foreign Intelligence Surveillance Act of 1978, As Amended," the "Presiding Judge of the Foreign Intelligence Surveillance Court," where available, assigns petitions received under section 501(f) of FISA to one of the FISC judges in the petition review pool. If the Presiding Judge of the FISC is unavailable, the local FISC judge with the most seniority, other than the Presiding Judge, becomes Acting Presiding Judge, and assigns the petition to an FISC judge in the petition review pool. If no local judge is available, the most senior FISC judge who is reasonably available becomes the Acting Presiding Judge, and makes the assignment of the petition.

If the judge does not find the petition frivolous, he or she has 72 hours in which to consider the petition and provide a written statement for the record of the reasons for any determination made. A petition to modify or set aside a directive may only be granted if the judge finds that the directive does not meet the requirements of section 105B or is otherwise unlawful. Otherwise the judge must immediately affirm the directive and order its recipient to comply with it. A directive not explicitly modified or set aside remains in full effect.[26] Within seven days of the assigned judge's decision, the government or a recipient of the directive may petition the Foreign Intelligence Surveillance Court of Review for review of that decision. The Court of Review must provide a written statement on the record of the reasons for its decision. The government or any recipient of the directive may seek review of the decision of the Court of Review by petition for a writ of certiorari to the U.S. Supreme Court.[27] All judicial proceedings under this section are to be concluded as expeditiously as possible.[28]

All petitions under this section are filed under seal. Upon request of the government in any proceeding under this section, the court shall review ex parte and in camera any government submission or portion of a submission which may contain classified information.[29] The record of all proceedings, including petitions filed, orders granted, and statements of reasons for decision, must be maintained under security measures established by the Chief Justice of the United States in consultation with the Attorney General and the DNI.[30] A directive made or an order granted under this section must be retained for at least ten years.[31]

Effect on or parallels to existing law. Section 105B is a new section added to title I of FISA, 50 U.S.C. §§ 1801 *et seq*. It differs from the other provisions of title I of FISA in that it does not deal with electronic surveillance, but rather with acquisitions that do not constitute electronic surveillance. Because section 105B does not specify where such acquisitions may occur or from whom, it appears that such foreign intelligence information concerning persons reasonably believed to be outside the United States may be acquired, at least in part, from persons, including U.S. persons, who are located within the United States.[32]

---

[26] P.L. 110-55, Sec. 105B(h).

[27] P.L. 110-55, Sec. 105B(i).

[28] P.L. 110-55, Sec. 105B(j).

[29] P.L. 110-55, Sec. 105B(k).

[30] P.L. 110-55, Sec. 105B(j).

[31] P.L. 110-55, Sec. 105B(m).

[32] It may be noted that the description of an acquisition under section 105B of FISA appears broad enough to encompass future collection of phone calling records for pattern analysis, but does not appear intended to address any past use of such investigative techniques. *Cf.*, Hepting v. AT&T Corp., 439 F. Supp. 2d. 974 (N.D. Cal. 2006); In re: National Security Agency Telecommunications Records Litigation, MDL No. 06-1791-VRW (March 13, 2007) (stipulation and order staying all cases except *Hepting* against AT&T Defendants); Hepting v. United States, Nos. 06-80109, 06-80110 (9th Cir. 2006) (order granting appeal).

Similar to electronic surveillance under section 102 of FISA, 50 U.S.C. § 1802, which may be authorized for up to one year by the President, through the Attorney General, without a court order if the Attorney General certifies in writing under oath that certain requirements are satisfied,[33] acquisitions under section 105B of FISA, may be authorized by the DNI and the Attorney General without a court order if they certify in writing under oath that certain criteria are met. However, section 105B has no parallel to section 102(a)(1)(B)'s requirement 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."

Similar to section 105B(d)'s reporting requirements, section 102(a)(2) requires electronic surveillance under that section to be carried out in accordance with the Attorney General's certification and applicable minimization requirements, and directs the Attorney General to assess compliance with "such procedures" and report his assessments to the House and Senate intelligence committees under the provisions of section 108(a) of FISA.

Section 102(a)(4), which permits the Attorney General to direct a specified communication common carrier to provide information, facilities, or technical assistance to the government needed to carry out the electronic surveillance involved and to compensate that communication common carrier at the prevailing rate for its aid, is structurally similar to section 105B(e) and (f). However, subsections 105B(e) and (g)-(i) permit the Attorney General and the DNI to direct "a person," rather than a "specified communication common carrier," to "immediately" furnish such aid; provide authority for the Attorney General to seek the aid of the FISC to compel

---

[33] Section 102(a), 50 U.S.C. § 1802(a) provides:

> (a)(1) Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that —
>
> (A) the electronic surveillance is solely directed at —
>
> (i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title; or
>
> (ii) 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 defined in section 1801(a)(1), (2), or (3) of this title;
>
> (B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and
>
> (C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801(h) of this title; and
>
> if the Attorney General reports 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.

compliance with such a directive; give the recipient of the directive a right to challenge the legality of the directive before the petition review pool of the same court; and permit both the government and the recipient of the directive to appeal that court's decision. The authority to challenge the legality of such a directive and to appeal the decision appears modeled, to some degree, after the process set forth in section 501(f) of FISA, 50 U.S.C. § 1861(f), dealing with challenges to the legality of production and nondisclosure orders.

Unlike electronic surveillance pursuant to a court order sought under section 104 of FISA, 50 U.S.C. § 1804, and authorized under section 105 of FISA, 50 U.S.C. § 1805, where the government provides the FISC with specific categories of substantive information about the electronic surveillance involved upon which the court can base its determinations; the government submits certain procedures[34] for review to the FISC, but does not provide the court with substantive information about the acquisitions themselves.

Sec. 3. Submission to Court Review and Assessment of Procedures

Section 3 of the act creates a new section 105C of FISA, creating a review process for the procedures under which the government determines that acquisitions of foreign intelligence information from persons reasonably believed to be located outside the United States do not constitute electronic surveillance.

New Section 105C of FISA. "Submission to Court Review of Procedures"

Subsection 105C(a) requires the Attorney General, within 120 days of enactment of the act,[35] to submit to the FISC the procedures by which the government determines that acquisitions conducted pursuant to section 105B of the act do not constitute electronic surveillance.[36] The procedures are to be updated and submitted to the FISC annually. Within 180 days after enactment, the FISC must assess whether the government's determination under section 105B(1) of FISA that the

---

[34] Compare section 105B(a)(1) with section 105C.

[35] Under Sec. 6(a) of the act, except as otherwise provided, the amendments made by the act are to take effect immediately after the date of enactment of the act. Sec. 105C(a) states that it will take effect within 120 days of the effective date of the act. For purposes of Sec. 105C(a), that would be 120 days after enactment.

[36] Section 105B(1) on its face refers only to "reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States," and requires "such procedures [to be] subject to review of the [FISC] pursuant to section 105C of this Act." *See* footnote 11, *supra*, for further discussion of the seeming ambiguities in the statutory language of sections 105B and 105C with respect to the procedures to be reviewed by the FISC.

procedures are "reasonably designed to ensure that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance"[37] is clearly erroneous.[38]

If the FISC deems the government's determination not clearly erroneous, the court must enter an order approving the continued use of the procedures. On the other hand, if the government's determination is found to be clearly erroneous, new procedures must be submitted with 30 days or any acquisitions under section 105B implicated by the FISC order must cease.[39] Any order issued by the FISC under subsection 105C(c) may be appealed by the government to the Foreign Intelligence Surveillance Court of Review. If the Court of Review finds the FISC order was properly entered, the government may seek U.S. Supreme Court review through a petition for a writ of certiorari.[40] Any acquisitions affected by the FISC order at issue may continue throughout the review process.

Comparison of this provision with court review. The section 105C procedure review process is new and does not appear to have a parallel in the other provisions of FISA.

Other possible effects of new sections 105A, 105B, and 105C. The Terrorist Surveillance Program has been characterized as involving "intercepts of contents of communications where one . . . party to the communication is outside the United States" and the government has "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."[41] In a letter from the Attorney General to Senator Leahy and Senator Specter on January 17, 2007, the Attorney General indicated that, based upon classified orders issued by a judge of the Foreign Intelligence Surveillance Court (FISC), electronic

---

[37] There appears to be some ambiguity regarding the procedures referenced in section 105B(a) and section 105C of FISA. Section 105B permits the DNI and the Attorney General to authorize acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States if the DNI and the Attorney General determine, based upon information provided to them, "that — (a)(1) there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States, and such procedures will be subject to review of the Court pursuant to section 105C of this Act[.]" However, section 105C requires the Attorney General to submit to the FISC "the procedures by which the Government determines that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance." For further discussion, see 15, *supra.*

[38] Section 105C(b) of FISA, as added by P.L. 110-55, Sec. 3.

[39] Section 105C(c) of FISA, as added by P.L. 110-55, Sec. 3.

[40] Section 105C(d) of FISA, as added by P.L. 110-55, Sec. 3. If the Court of Review affirms the FISC order, the Court of Review must immediately prepare a written statement of each of the reasons for its decision. Should the government file a certiorari petition, that written record would be transmitted under seal to the U.S. Supreme Court.

[41] *See* Press Release, White House, Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (December 19, 2005).

surveillances previously carried out under the Terrorist Surveillance Program would thereafter be under the court's supervision. His letter stated, in part:

> I am writing to inform you that on January 10, 2007, a Judge of the Foreign Intelligence Surveillance Court issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization. As a result of these orders, any electronic surveillance that was occurring as part of the Terrorist Surveillance Program will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court....[42]

A question may arise as to whether new section 105A's interpretation of the definition of "electronic surveillance" under FISA, might impact the FISC's jurisdiction over some or all of the interceptions to which the Attorney General referred. Under section 103(a) of FISA, 50 U.S.C. § 1803(a):

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

Section 102(b) of FISA, 50 U.S.C. § 1802(b), provides that:

> Applications for a court order under [title I of FISA, 50 U.S.C. §§ 1801 *et seq*.] are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the court having jurisdiction under section 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 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.

The answer to the jurisdictional question raised above would seem to depend on whether those interceptions were directed at the communications of a person reasonably believed to be located outside the United States. If so, then, by virtue of section 105A, such interceptions would not be construed to fall within the definition of "electronic surveillance" under FISA, and therefore a review of the underpinnings of such interceptions would not be within the FISC's jurisdiction in connection with an application to authorize electronic surveillance. If treated instead as acquisitions

---

[42] 153 *Cong. Rec*. S646-S647 (January 17, 2007) (Letter of Attorney General Alberto Gonzales to the Chairman and Ranking Member of the Senate Judiciary Committee ordered printed, without objection, in the *Record* during Senator Leahy's remarks on the FISA Program).

under new section 105B of FISA, then the FISC would seem to be limited to reviewing, under a clearly erroneous standard, the general procedures under which the Director of National Intelligence (DNI) and the Attorney General would make determinations that acquisitions did not constitute electronic surveillance;[43] and judges of the FISC petition review pool would have jurisdiction to consider petitions challenging the legality of directives to persons to furnish aid to the government to accomplish those acquisitions.[44]

Implicit in the previous discussion is the question what impact, if any, any possible narrowing of the interpretation of the definition of "electronic surveillance" under FISA might have upon the scope of "acquisitions" under new section 105B of FISA. In other words, if an interception of communications directed toward a person reasonably believed to be located outside the United States does not constitute "electronic surveillance" for purposes of FISA, regardless of where the other parties to the communication may be located or whether some or all of those other parties may be U.S. persons, could some or all such interceptions be deemed "acquisitions" under the provisions of section 105B?

For this to be the case, it would appear that the interception would have to be authorized by the DNI and the Attorney General under section 105B of FISA to acquire foreign intelligence information concerning persons reasonably believed to be outside the United States, and would have to satisfy the five criteria set forth in section 105B(a), including the use of minimization procedures.[45] If these requirements are met, then it appears that some communications to which U.S. persons located within the United States might be parties could be intercepted for periods of up to one year without a court order under section 105B.

This contrasts markedly with the detailed information to be provided by the government to the FISC in an application for a court order for electronic surveillance under section 104 of FISA, 50 U.S.C. § 1804,[46] and the level of FISC review provided for such applications. To the extent that new section 105A circumscribes

---

[43] Section 105C(a) of FISA, as added by P.L. 110-55, Sec. 3.

[44] Section 105B(h) of FISA, as added by P.L. 110-55, Sec. 2.

[45] Section 105B(a)(5) of FISA, as added by Sec. 2 of P.L. 110-55. For further discussion of minimization procedures in section 105B(a)(5), see footnote 12, *supra*, and accompanying text. Under section 105(f) of FISA, 50 U.S.C. § 1805(f), in approving an application for electronic surveillance under FISA, an FISC judge must find, in part, that the proposed minimization procedures applicable to that surveillance meet the definition of minimization procedures under section 101(h) of FISA, 50 U.S.C. § 1801(h). In authorizing an acquisition under section 105B, the DNI and the Attorney General must certify in writing under oath, in part, that "the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h)."

[46] Section 104 of FISA, 50 U.S.C. § 1804, which deals with application for FISC court orders authorizing electronic surveillance, requires eleven categories of detailed information to be submitted by a federal office in writing under oath or affirmation to an FISC judge. Each application must be approved by the Attorney General based upon his finding that the application satisfies the criteria and requirements set forth in title I of FISA. Section 105 of FISA, 50 U.S.C. § 1805, sets out the findings that a FISC judge must make in approving such an application.

the previous interpretation of "electronic surveillance" as defined under section 101(f) of FISA, 50 U.S.C. § 1801(f), it could be argued that this might significantly diminish the degree of judicial review to which such interceptions might have heretofore been entitled. On the other hand, if the interpretation of the definition of "electronic surveillance" contemplated in new section 105A of FISA is consistent with prior practice, then this concern with respect to section 105A's impact would appear to be eliminated.

A somewhat closer parallel might be drawn between the statutory structure for acquisitions contemplated in section 105B and that for electronic surveillance under section 102 of FISA, 50 U.S.C. § 1802. The latter section permits the President, through the Attorney General, to authorize electronic surveillance for up to one year without a court order, if the Attorney General certifies in writing under oath that the electronic surveillance is solely directed at the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title;[47] or the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of such a foreign power. In addition, the Attorney General must 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; and that the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801(h) of this title; and he must comply with reporting requirements regarding those minimization procedures.

Subsection 102(b) of FISA denies the FISC jurisdiction to grant any order approving electronic surveillance directed solely at the acquisition of communications used exclusively between or among such foreign powers or the acquisition of such technical intelligence from property or premises under the exclusive and open control of such foreign powers, *unless such surveillance may involve the acquisition of communications of any United States person.* Section 105B provides the FISC no similar jurisdiction if an acquisition involves the communications of a United States person. Again, if the interpretation of the definition of "electronic surveillance" contemplated in new section 105A of FISA is consistent with prior practice, then this concern regarding section 105A's effect would appear to be eliminated.

To the extent that any intentional interceptions of communications which were previously deemed to be covered by the definition of "electronic surveillance" under FISA are now excluded from that definition, another question which may arise is whether any of those interceptions may now be found to fall within the general prohibition against intentional interception of wire, oral, or electronic communications under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 U.S.C. § 2511. Under 18 U.S.C. § 2511(2)(f), "electronic surveillance," as defined in section 101 of the Foreign Intelligence Surveillance Act,

---

[47] *See* footnote 6, *supra*, for the definition of "foreign power" under section 101(a)(1), (2), or (3) of FISA.

is an exception to this general prohibition.[48] If such interceptions were deemed to violate 18 U.S.C. § 2511, then the intentional use or disclosure of the contents of such communications, knowing that the information was obtained through the interception of a wire, oral, or electronic communication in violation of 18 U.S.C. § 2511 would also be prohibited under that section.

Sec. 4. Reporting to Congress

Section 4 of P.L. 110-55 requires the Attorney General to inform the Senate Select Committee on Intelligence, the House Permanent Select Committee on Intelligence, the Senate Judiciary Committee and the House Judiciary Committee semi-annually concerning acquisitions "under this section"[49] during the previous six-month period. Each report is to include descriptions of any incidents of non-compliance with a directive issued by the DNI and the Attorney General under section 105B, including noncompliance by an element of the Intelligence Community with guidelines or procedures for determining that "the acquisition of foreign intelligence authorized by the Attorney General and the [DNI] concerns persons reasonably to be outside the United States,"[50] and incidents of noncompliance by a specified person to whom a directive is issued under section 105B. The report is also required to include the number of certifications and directives issued during the reporting period.

Sec. 5. Technical Amendment and Conforming Amendments

Section 5(a)(1) and (a)(2) make technical amendments to section 103(e)(1) and (2) of FISA, 50 U.S.C. § 1803(e)(1) and (2), to reflect the jurisdiction of the FISC petition review pool over petitions under section 105B(h) of FISA, dealing with challenges to the legality of directives issued under section 105B(e) of FISA to a person by the Attorney General and the DNI, and over petitions under section 501(f)[51]

---

[48] If there are any types of intentional interceptions of communications previously covered by FISA's definition of electronic surveillance, which may now be prohibited under 18 U.S.C. § 2511, this, in turn, might give rise to the question whether, if the President were to carry out such interceptions under an assertion of his constitutional authority under Article II, the application of Title III's prohibition to those interceptions would be found by a court to be unconstitutional, or whether the application of this prohibition to such interceptions would withstand constitutional scrutiny. *Cf.*, In re Sealed Case, 310 F. 3d 717, 742, 746 (U.S. Foreign Intell. Surveillance Ct. Rev. 2002).

[49] This appears to be a reference to section 105Bof FISA, as added by P.L.110-55, Sec. 2.

[50] This may be intended to read "the acquisition of foreign intelligence *information* authorized by the Attorney General and Director of National Intelligence concerns persons reasonably *believed* to be outside the United States." (Emphasis added.)

[51] Sec. 5(a)(1) and (2) of the act refer here to section "501(f)(1)," rather than to section "501(f)," of FISA. The reference to section 501(f)(1) of FISA, 50 U.S.C. § 1861(f)(1), may be intended to be a reference to section 501(f), 50 U.S.C. § 1861(f). Section 501(f), as

(continued...)

of FISA, 50 U.S.C. § 1861, dealing with challenges to production orders or nondisclosure orders issued by the FISC under section 501(c) of FISA, 50 U.S.C. § 1861(c).

Section 5(b) makes conforming amendments to the table of contents of the first "section"[52] of FISA, 50 U.S.C. § 1801 *et seq.*, to reflect the additions of new sections 105A, 105B, and 105C of FISA.

Sec. 6. Effective Date; Transition Procedures

Effective Date

Under Section 6(a) of P.L. 110-55, the amendments to FISA made in the act are to take effect immediately after its enactment except as otherwise provided.

Transition Procedures

Section 6(b) of P.L. 110-55 provides that any order issued under FISA in effect on the date of enactment of P.L. 110-55 (August 5, 2007) shall remain in effect until the date of expiration of the order, and, at the request of the applicant for the order, the FISC shall reauthorize the order as long as the facts and circumstances continue to justify its issuance under FISA as in effect the day before the applicable effective date of P.L. 110-55. This appears to refer to orders and applications for orders under FISA authorizing electronic surveillance,[53] physical searches,[54] pen registers or trap and trace devices,[55] or production of tangible things and related nondisclosure orders.[56]

---

[51] (...continued)
added to FISA by P.L. 109-177, § 106(f), was rewritten by P.L. 109-178, § 3. Current section 501(f)(1) of FISA contains two subsections, defining the terms "production order" and "nondisclosure order," respectively, for purposes of section 501. For further discussion, see footnote 24, *supra*.

[52] This appears to be intended to refer to the title I of FISA, dealing with electronic surveillance.

[53] Applications for electronic surveillance are covered by section 104 of FISA, 50 U.S.C. § 1804, while orders authorizing such surveillance are addressed in section 105 of FISA, 50 U.S.C. § 1805. These sections were not amended by P.L.110-55.

[54] Applications for physical searches are addressed in sections 302(b) and 303 of FISA, 50 U.S.C. §§ 1822(b) and 1823, while orders authorizing such physical searches are addressed in section 304 of FISA, 50 U.S.C. § 1824. These sections were not amended by P.L.110-55.

[55] Applications for installation and use of pen registers and trap and trace devices are addressed in subsections 402(a), (b), and (c) of FISA, 50 U.S.C. § 1842(a), (b), and (c); while orders authorizing installation and use of such pen registers and trap and trace devices are covered by subsection 402(d), 50 U.S.C. § 1842(d). No amendments to these subsections were made in P.L. 110-55.

[56] Applications for orders "requiring the production of any tangible things (including books, (continued...)

Section 6(b) provides further that the government may also file new applications and the FISC shall enter orders granting such applications pursuant to FISA, as long as the application meets the requirements set forth in FISA as in effect on the day before the applicable effective date of P.L. 110-55. This seems to indicate that pre-existing authorities under FISA remain available in the wake of P.L. 110-55's enactment. At the applicant's request, the FISC shall extinguish any extant authorizations to conduct electronic surveillance or physical searches pursuant to FISA. Any surveillance conducted pursuant to an order entered under subsection 6(b) of P.L. 110-55 is to be subject to the provisions of FISA as in effect before the effective date of P.L. 110-55.

Under Section 6(c) of P.L. 110-55, sections 2, 3, 4, and 5 of that act were to sunset 180 days after the date of enactment of the act, except as provided in section 6(d). Under section 6(d), any authorizations for acquisition of foreign intelligence information or directives issued pursuant to those authorizations issued under section 105B shall remain in effect until their expiration. Section 6(d) also provides that such acquisitions shall be governed by the applicable amendments made to FISA by P.L. 110-55, and shall not be deemed to constitute electronic surveillance as that term is defined in section 101(f) of FISA.[57]

On January 29, 2008, both the House and the Senate passed H.R. 5104, a 15-day extension to the sunset for the Protect America Act, to allow further time to consider, pass, and go to conference on proposed legislation to amend FISA, while ensuring that the intelligence community would have the authority it needed in the intervening period. It was signed into law on January 31, 2008, as P.L. 110-182. On February 13, 2008, the House rejected H.R. 5349, which would have extended the sunset provision for an additional 21 days. Bills have been introduced in the Senate to extend the sunset from 180 to 210 days (S. 2541, S. 2556, and S. 2615), or to extend it to July 1, 2009 (S. 2557). The President has indicated that he will not agree to a further extension of the sunset provision.[58]

---

[56] (...continued)
records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution" are addressed in subsections 501(a) and (b) of FISA, 50 U.S.C. § 1861(a) and (b). Production orders are covered in subsection 501(c) of FISA, 50 U.S.C. § 1861(c), while related nondisclosure orders are addressed in subsection 501(d) of FISA, 50 U.S.C. § 1861(d). These subsections were not amended by P.L. 110-55.

[57] The provisions in section 6(c) and (d) were added by Senate amendment 2649 to S. 1927, proposed by Senator McConnell, for himself and Senator Bond. It was agreed to by unanimous consent on August 3, 2007. As amended, the bill passed the Senate by Yea-Nay vote, 60-28 (Record Vote Number 309), 153 *Cong. Rec*. S10861-S10872 (August 3, 2007).

[58] Speech by President Bush on the Protect America Act (February 13, 2008), available at [http://www.whitehouse.gov/news/releases/2008/02/20080213.html].