Order Code RL33669



# Terrorist Surveillance Act of 2006: S. 3931 and Title II of S. 3929, the Terrorist Tracking, Identification, and Prosecution Act of 2006

**September 25, 2006**

Elizabeth B. Bazan
Legislative Attorney
American Law Division

# Terrorist Surveillance Act of 2006: S. 3931 and Title II of S. 3929, the Terrorist Tracking, Identification, and Prosecution Act of 2006

## Summary

On Friday, September 22, 2006, two bills were introduced by Senator Mitch McConnell, for himself and Senator William H. Frist, that deal with foreign intelligence surveillance: S. 3931, the "Terrorist Surveillance Act of 2006," and S. 3929, the "Terrorist Tracking, Identification, and Prosecution Act of 2006," Title II of which parallels S. 3931. The bills would create a new Title VII of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA), 50 U.S.C. § 1801 *et seq.*, to address electronic surveillance programs. In addition, the measures would amend other provisions of FISA dealing with electronic surveillance without a warrant pursuant to an Attorney General certification, applications for a Foreign Intelligence Surveillance Court orders authorizing electronic surveillance for foreign intelligence purposes, the contents of such orders, emergency electronic surveillance under FISA, limitations on liability for those who aid the federal government in connection with electronic surveillance to obtain foreign intelligence information, and applicable congressional oversight. The bills would repeal the current wartime authorities for electronic surveillance without a warrant following a congressional declaration of war. Changes would be made to the FISA definitions of "electronic surveillance" and "agent of a foreign power," among others. Other provisions would modify the criminal provisions of FISA and the exclusivity clause 18 U.S.C. § 2511(2)(f). Still other provisions amend FISA to address those who engage in the development or proliferation of weapons of mass destruction and to accommodate the international movements of targets of electronic surveillance under FISA.

This report discusses the provisions of S. 3931 and Title II of S. 3929, and notes the changes to existing law that these measures would make if enacted.

## Contents

# Terrorist Surveillance Act of 2006: S. 3931 and Title II of S. 3929, the Terrorist Tracking, Identification, and Prosecution Act of 2006

## Introduction

The "Terrorist Surveillance Act of 2006" was introduced by Senator Mitch McConnell, for himself and Senator William H. Frist, on Friday, September 22, 2006, as a free-standing bill, S. 3931. On the same day, Senator McConnell, for himself and Senator Frist, introduced S. 3929, the "Terrorist Tracking, Identification and Prosecution Act of 2006,"[1] Title II of which is the "Terrorist Surveillance Act of 2006." These are the latest in a series of Senate bills addressing the authorization, review, and oversight of electronic surveillance programs designed to acquire foreign intelligence or to provide information to assist in detecting and preventing international terrorist threats to the United States.

S. 3931 and Title II of S. 3929 would create a new Title VII of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA), 50 U.S.C. § 1801 *et seq.*, to address electronic surveillance programs. In addition, the measures would amend other provisions of FISA dealing with electronic surveillance without a warrant pursuant to an Attorney General certification, applications for a Foreign Intelligence Surveillance Court orders authorizing electronic surveillance for foreign intelligence purposes, the contents of such orders, emergency electronic surveillance under FISA,

---

[1] S. 3931 and Title II of S. 3929 appear to be substantively identical, but for differences in section numbers, with one exception. In Sec. 205 of S. 3929, new Section 703 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA), which sets out the requirements for an application for Foreign Intelligence Surveillance Court (FISC) authorization of electronic surveillance programs, there are two identical new subsections 703(a)(9) of FISA. Each indicates that such an application shall "include a statement of the proposed minimization procedures[.]" Sec. 5 of S. 3931 does not have this duplication of the subsection. In S. 3929, the "Terrorist Surveillance Act of 2006" was combined with Title I of that bill, the "Military Commission Act of 2006." The "Military Commission Act of 2006" was also introduced on September 22, 2006, as a free-standing measure, S. 3930. For further information on military commission and detainee issues, see CRS Report RL31600, *The Department of Defense Rules for Military Commissions: Analysis of Procedural Rules and Comparison with Proposed Legislation and the Uniform Code of Military Justice*, by Jennifer K. Elsea; CRS Report RL33180, *Enemy Combatant Detainees: Habeas Corpus Challenges in Federal Court*, by Jennifer K. Elsea and Kenneth Thomas; CRS Report RL33655, *Interrogation of Detainees: Overview of the McCain Amendment*, by Michael John Garcia; and CRS Report RL33662, *The War Crimes Act: Current Issues*, by Michael John Garcia.

limitations on liability for those who aid the federal government in connection with electronic surveillance to obtain foreign intelligence information, and applicable congressional oversight. The bills would repeal the current wartime authorities for electronic surveillance without a warrant following a congressional declaration of war. Changes would be made to the FISA definitions of "electronic surveillance" and "agent of a foreign power," among others. Other provisions would modify the criminal provisions of FISA and the exclusivity clause 18 U.S.C. § 2511(2)(f). Still other provisions amend FISA to address those who engage in the development or proliferation of weapons of mass destruction and to accommodate the international movements of targets of electronic surveillance under FISA. This report will discuss the substantive provisions of the "Terrorist Surveillance Act of 2006" and their impact on existing law.

# Summary of Changes to Existing Law

## New Title VII of the Foreign Intelligence Surveillance Act (FISA) — Electronic Surveillance Programs

**Foreign Intelligence Surveillance Court (FISC) Jurisdiction.** Sec. 3 of S. 3931, Sec. 203 of S. 3929, creates a new Title VII[2] in FISA, which deals with electronic surveillance programs. "Electronic surveillance program" is defined under the new Section 701 of FISA to mean "a program to engage in electronic surveillance":

> (A) that has as a significant purpose the gathering of foreign intelligence information[3] or protecting against international terrorism;
> (B) where it is not feasible to name every person, address, or location to be subjected to electronic surveillance;

---

[2] The current Title VII of FISA would then be redesignated Title VIII.

[3] "Foreign intelligence information" is defined in new Sec. 701(4) of FISA to have "the same meaning as in section 101(e) of FISA [current 50 U.S.C. § 1801(e),], and includes information necessary to protect against international terrorism." Currently, under FISA, the term means:

> (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.

> (C) where effective gathering of foreign intelligence information requires the flexibility to begin electronic surveillance immediately after learning of suspect activity; and
> (D) where effective gathering of foreign intelligence information requires an extended period of electronic surveillance.

Under Sec. 4 of S. 3931, Sec. 204 of S. 3929, a new Section 702(a) of FISA would vest jurisdiction in the FISC to review, authorize, and reauthorize such electronic surveillance programs to obtain foreign intelligence information or to protect against international terrorism. Under this subsection, an initial authorization of an electronic surveillance program may be for up to 90 days, while a reauthorization may be for a period of time not longer than the FISC determines to be reasonable. If the FISC denies an application for authorization or reauthorization of an electronic surveillance program, the Attorney General may submit an unlimited number of new applications seeking approval of the program or, in the alternative, may appeal the decision of the FISC to the Foreign Intelligence Surveillance Court of Review (FIS Court of Review).

If, at any time, the Attorney General determines that the known facts and circumstances relating to any target within the United States who is being surveilled under Title VII of FISA satisfy the criteria for an application for electronic surveillance of that target under Section 104 of Title I of FISA, 50 U.S.C. § 1804, then the Attorney General would be required to discontinue the surveillance of that target under the electronic surveillance program authorized under Title VII of FISA, unless certain conditions are met. The Attorney General could continue surveillance under Title VII only if, as soon as he determines practicable after he makes the determination to continue the surveillance of the target under Title VII, he makes an application under Section 104 of FISA for an FISC order authorizing electronic surveillance of the target under Section 105 of FISA, 50 U.S.C. § 1805. New Section 702(a)(4) of FISA, Sec. 4(a) of S. 3931, Sec. 204(a) of S. 3929.

**Mandatory transfer of certain cases.** The bills also authorize the transfer from any other court of cases involving a challenge to the legality of classified communications intelligence activity relating to a foreign threat, including an electronic surveillance program, or cases in which the legality of any such activity or program is at issue. Such a transfer would be triggered by the filing by the Attorney General of an affidavit under oath that the case should be transferred to the FIS Court of Review, because further proceedings in the originating court would harm the national security of the United States. Under the proposed language in new Section 702(b)(1) of FISA, Sec. 4(a) of S. 3931, Sec. 204(a) of S. 3929, when such an affidavit is filed, originating court must transfer the case. While the implication of the Attorney General's affidavit may be that the transfer from the originating court would be to the FIS Court of Review, this is not clear from the language of proposed subsection 702(b)(1), which states "the originating court shall transfer the case of the Foreign Intelligence Surveillance for further proceedings under this subsection." As written, it appears that some words may be missing from this clause.

This uncertainty is increased by the language in proposed subsection 702(b)(2) of FISA, entitled "Procedures for Review." In this subsection, the FISC, rather than the FIS Court of Review, is given jurisdiction as appropriate to determine standing

and to determine the legality of the program to the extent necessary for resolution of the underlying case.[4] If the FISC determines, in the context of a criminal proceeding, that the U.S. Constitution would require disclosure of national security information, any such disclosure would be governed by the Classified Information Procedures Act, 18 U.S.C. App. 3, or, if applicable, 18 U.S.C. § 2339B(f).[5] Under proposed subsection 702(b)(3), entitled, "Appeal, Certiorari, and Effects of Decisions," any decision of the FISC under proposed subsections 702(b)(1) and (2) would be subject to review by the FIS Court of Review under section 103(b) of FISA, 50 U.S.C. § 103(b).[6] Under new subsection 702(b)(3), the United States may seek review of

---

[4] Subsection 702(b)(2) indicates that "all proceedings under this paragraph" are to be conducted in accordance with the procedures set forth in Section 106(f) of FISA, 50 U.S.C. § 1806(f), which currently provides:

> (f) In camera and ex parte review by district court
>
> Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

[5] The Classified Information Procedures Act, 18 U.S.C. App. 3, and 18 U.S.C. § 2339B(f) provide procedures for the use and handling of classified procedures in the context of criminal proceedings and civil proceedings brought by the United States under 18 U.S.C. § 2339B, respectively.

[6] Current Section 103(b) of FISA deals with the creation of the FIS Court of Review, to which is given jurisdiction to review a denial of an application for a court order under FISA. If the FIS Court of Review determines that an application was properly denied, the United States Government may seek review of the denial on petition for a writ of certiorari to the U.S. Supreme Court. It states:

> (b) Court of review; record, transmittal to Supreme Court
>
> The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a court of review which shall have jurisdiction to review the denial of any application made under this chapter.

(continued...)

decisions by the FIS Court of Review on certiorari to the U.S. Supreme Court. Otherwise, the decision of the FISC would be binding in all other courts.

Under new subsection 702(b)(4), the FISC or the originating court may dismiss a challenge to the legality of an electronic surveillance program for any reason provided for under law. All litigation privileges are preserved under new subsection 702(b)(5).

**Applications for approval of electronic surveillance programs.** Under Sec. 5 of S. 3931, Sec. 205 of S. 3929, a new Section 703 of FISA is created, which sets out the requirements for applications for approval of electronic surveillance programs, including resubmission of applications or applications for reauthorization of such programs.[7] Subsection 703(b) authorizes the FISC to require

---

[6] (...continued)

> If such court determines that the application was properly denied, the court shall immediately provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

[7] Such an application would be:

> (1) made by the Attorney General or his designee;
> (2) include a statement of the authority conferred on the Attorney General by the President of the United States;
> (3) include a statement setting forth the legal basis for the conclusion by the Attorney General that the electronic surveillance program is consistent with the Constitution of the United States;
> (4) certify that a significant purpose of the electronic surveillance program is to obtain foreign intelligence information or to protect against international terrorism;
> (5) certify that the information sought cannot reasonably be obtained by normal investigative techniques[;]
> (6) certify that the information sought cannot reasonably be obtained through an application under section 104;
> (7) include a statement of the means and operational procedures by which the electronic surveillance will be executed and effected;
> (8) include an explanation of how the electronic surveillance program is reasonably designed to ensure that the communications that are acquired are communications of or with —
>
> > (A) a foreign power that engages in international terrorism or activities in preparation therefor;
> > (B) an agent of a foreign power that engages in international terrorism or activities in preparation therefor;
> > (C) a person reasonably believed to have communication with or be associated with a foreign power that engages in international terrorism or activities in preparation therefor or an agent of a foreign power that engages in international terrorism or activities in preparation therefor; or
> > (D) a foreign power that poses an imminent threat of attack likely to cause death, serious injury, or substantial economic damage to the United States, or an agent of a foreign power thereof;

(continued...)

the Attorney General to furnish such other information as may be necessary for the court to make a determination under new section 704.

**Approval of electronic surveillance programs by the FISC.** Sec. 6 of S. 3931, Sec. 206 of S. 3929, creates a new subsection 704 addressing the necessary findings for and contents of an ex parte FISC order approving an electronic surveillance program as requested or as modified.[8] In part, the court must find that approval of the electronic surveillance program in the application is consistent with the U.S. Constitution. New subsection 704(b) of FISA identifies the factors which

---

[7] (...continued)

(9) include a statement of the proposed minimization procedures;
(10) if the electronic surveillance program that is the subject of the application was initiated prior to the date the application was submitted, specify the date that the program was initiated;
(11) include a description of all previous applications that have been made under this title involving the electronic surveillance program in the application (including the minimization procedures and the means and operations procedures proposed) and the decision on each previous application; and
(12) include a statement of facts concerning the implementation of the electronic surveillance program described in the application, including, for any period of operation of the program authorized not less than 90 days prior to the date of submission of the application —

(A) the minimization procedures implemented; and
(B) the means and operational procedures by which the electronic surveillance was executed and effected.

[8] The FISC must find that:

(1) the President has authorized the Attorney General to make the application for electronic surveillance for foreign intelligence information or to protect against international terrorism;
(2) approval of the electronic surveillance program in the application is consistent with the Constitution of the United States;
(3) the electronic surveillance program is reasonably designed to ensure that the communications that are acquired are communications of or with —

(A) a foreign power that engages in international terrorism or in activities in preparation therefor;
(B) an agent of a foreign power that is engaged in international terrorism or in activities in preparation therefor;
(C) a person reasonably believed to have communication with or be associated with a foreign power that is engaged in international terrorism or in activities in preparation therefor or an agent of a foreign power that is engaged in international terrorism or in activities in preparation therefor; or
(D) a foreign power that poses an imminent threat of attack likely to cause death, serious injury, or substantial economic damage to the Untied States, or an agent of a foreign power thereof;

(4) the proposes minimization procedures meet the definition of minimization procedures under section 101(h); and
(5) the application contains all statements and certifications required by section 703.

the FISC may consider in assessing the constitutionality of the program.[9] Subsection 704(c) of FISA sets out the contents of an order approving such a program.[10]

**Congressional oversight of electronic surveillance programs authorized under new Title VII of FISA.** Under Sec. 7 of S. 3931, Sec. 207 of S. 3929, new Sec. 705 of FISA addresses congressional oversight. The Attorney General is directed to submit a classified report at least every 180 days to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence (the "congressional intelligence committees," as defined in new Sec. 701(2) of FISA) on the activities during the previous 180 day period under any electronic surveillance program authorized under new Title VII of FISA.[11] Under

---

[9] Such factors include:

> (1) whether the electronic surveillance program has been implemented in accordance with the proposal by the Attorney General, by comparing —
>
> (A) the minimization procedures proposed with the minimization procedures actually implemented;
>
> (B) the nature of the information sought with the nature of the information actually obtained; and
>
> (C) the means and operational procedures proposed with the means and operational procedures actually implemented; and
>
> (2) whether foreign intelligence information has been obtained through the electronic surveillance program.

[10] Under proposed subsection 704(c), an order approving an electronic surveillance program under this section shall direct —

> (1) that the minimization procedures be followed;
>
> (2) that, upon the request of the applicant, specified communication or other common carriers, landlords, custodians, or other specified persons, furnish the applicant forthwith with all information, facilities, or technical assistance necessary to undertake the electronic surveillance program in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carriers, landlords, custodians, or other persons are providing potential targets of the electronic surveillance program;
>
> (3) that any records concerning the electronic surveillance program or the aid furnished or retained by such carriers, landlords, custodians, or other persons are maintained under security procedures approved by the Attorney General and the Director of National Intelligence; and
>
> (4) that the applicant compensate, at the prevailing rate, such carriers, landlords, custodians, or other persons for furnishing such aid.

[11] Each report shall include a description of —

> (1) the minimization procedures implemented;
>
> (2) the means and operational procedures by which the electronic surveillance program was executed and effected;
>
> (3) significant decisions of the Foreign Intelligence Surveillance Court on applications made under section 703;
>
> (4) the total number of applications made for orders approving electronic surveillance programs pursuant to this title; and

(continued...)

subsection 705(c), "Nothing in this title shall be construed to limit the authority or responsibility of any committee of either House of Congress to obtain such information as such committee may need to carry out its respective functions and duties."

## Clarification of the Foreign Intelligence Surveillance Act of 1978

Sec. 8 of S. 3931, Sec. 208 of S. 3929, makes a series of amendments to FISA.

**Repeal of wartime authorities under FISA.** Sec. 8(a) of S. 3931, Sec. 208(a) of S. 3929, repeals Sections 111, 309, and 404 of FISA, 50 U.S.C. §§ 1811, 1829, and 1844, which respectively permit the President, through the Attorney General, to authorize electronic surveillance, physical searches, and the use of pen register or trap and trace devices, without a court order to obtain foreign intelligence information for up to 15 calendar days following a declaration of war by Congress.

**Clarifying amendments to 18 U.S.C. §§2511(2)(e) and (f) and to criminal provisions in Section 109 of FISA.** In general, 18 U.S.C. § 2511 prohibits the interception of wire, oral, or electronic communications unless the interception falls within one of a series of specific exceptions. Current 18 U.S.C. §§ 2511(2)(e) and (2)(f) set out two of these exceptions.

***Amendment to 18 U.S.C. § 2511(2)(e).*** Current 18 U.S.C. § 2511(2)(e) provides, "Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act." As amended, subsection 2511(2)(e) would read, "Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance under the Constitution or the Foreign Intelligence Surveillance Act of 1978."

***Amendment to 18 U.S.C. § 2511(2)(f).*** Current 18 U.S.C. § 2511(2)(f), often referred to as the "exclusivity" provision, states:

> (f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than

---

[11] (...continued)

> (5) the total number of orders applied for that have been granted, modified, or denied.

> electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

Thus, under the current exclusivity provision in 18 U.S.C. § 2511(2)(f), electronic surveillance is prohibited except when carried out under the provisions of FISA; chapter 119, 18 U.S.C. §§ 2510 *et seq*. (which deals with interception of wire, oral, or electronic communications); or chapter 121, 18 U.S.C. §§ 2701 *et seq*. (which deals with stored wire and electronic communications and transactional records access). As amended, 18 U.S.C. § 2511(2)(f) would read, "Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information that is authorized under a Federal statute or the Constitution of the United States."

***Amendments to Section 109 of FISA.*** The amendments to FISA in Sec.8(b)(2) of S. 3931, Sec. 208(b)(2) of S. 3929, address Section 109 of FISA, 50 U.S.C. § 1809, which currently provides criminal sanctions for any person who intentionally "(1) engages in electronic surveillance under color of law except as authorized by statute; or (2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute." As amended by Sec. 8(b)(2)(A) of S. 3931, Sec. 208(b)(2)(A) of S. 3929, a person would face criminal liability if he or she: (1) intentionally engages in electronic surveillance under color of law except as authorized by *law*; (2) intentionally discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by *law*; or (3) "*knowingly discloses or uses information obtained under color of law by electronic surveillance in a manner or for a purpose not authorized by law*." (Italics indicate new language.) Under Sec. 8(b)(2)(B) of S. 3931, Sec. 208(b)(2)(B) of S. 3929, the current penalties provided in Sec. 109(c) of FISA, 50 U.S.C. § 1809(c) would be increased from a fine of up to $10,000 to a fine of up to $100,000, while imprisonment would be increased from a term of up to 5 years to imprisonment for up to 15 years.

## Modernizing Amendments to FISA

Sec. 9 of S. 3931, Sec. 209 of S. 3929, makes several additional amendments to FISA.

**Definitions.** Sec. 9(b) of S. 3931, Sec. 209(b) of S. 3929, amends several of the definitions in Sec. 101 of FISA, 50 U.S.C. § 1801.

***Agent of a foreign power.*** Sec. 9(b)(1) of S. 3931, Sec. 209(b)(1) of S. 3929, expands the definition of "agent of a foreign power" under Sec. 101(b)(1) of

FISA, 50 U.S.C. § 1801(b)(1), to include a person other than a United States person[12] who "otherwise is reasonably expected to possess, control, transmit, or receive foreign intelligence information while that person is in the United States, provided that the official making the certification required in section 104(a)(6) deems such foreign intelligence information to be significant." This definition would become subsection 101(b)(1)(D) of FISA, 50 U.S.C. § 1801(b)(1)(D).

***Electronic surveillance.*** Sec. 9(b)(2) of S. 3931, Sec. 209(b)(2) of S. 3929, deletes the current definition of "electronic surveillance" under Sec. 101(f) of FISA,

---

[12] "United States person" is currently defined in Sec. 101(i) of FISA, 50 U.S.C. § 1801(i), to mean

> 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 (a)(1), (2), or (3) of this section.

A "foreign power" as defined in subsections 101(a)(1), (2) or (3) of FISA, 50 U.S.C. § 1801(a)(1), (2), or (3) includes "(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;" or "(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments."

50 U.S.C. § 1801(f),[13] and replaces it with a new definition. Under the new definition, "electronic surveillance" would mean:

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

This appears to be a shorter, but more expansive definition than that under current law.

***Minimization procedures with respect to electronic surveillance.*** Minimization procedures under FISA are designed to minimize the acquisition and retention, and prohibit the dissemination of non-publicly available information regarding unconsenting U.S. persons acquired during the course of electronic surveillance or physical search for foreign intelligence purposes, consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. Such procedures permit retention and dissemination to law enforcement of evidence of criminal activity. Under these procedures, nonpublicly available information which is not foreign intelligence information shall not be disseminated

---

[13] Under current Sec. 101(f) of FISA, 50 U.S.C. § 1801(f), "electronic surveillance" is defined 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.

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. Current Sec. 101(h)(4) of FISA, 50 U.S.C. § 1801(h)(4), also includes minimization procedures applicable to any electronic surveillance without a court order to acquire foreign intelligence information upon Attorney General certification pursuant to Sec. 102(a) of FISA, 50 U.S.C. § 1802. In that context, minimization procedures also encompass procedures requiring that no contents of any communication to which a United States person is a party be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under Sec. 105 of FISA, 50 U.S.C. § 1805, is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person. Subsection 104(h)(4) of FISA, 50 U.S.C. § 1801(h)(4), would be deleted by Sec. 9(b)(3) of S. 3931, Sec. 209(b)(3) of S. 3929, and replaced with new language under which minimization procedures would include:

> (4) notwithstanding paragraphs (1), (2), and (3) [of Section 104(h) of FISA, 50 U.S.C. § 1804(h)], with respect to any electronic surveillance approved pursuant to section 102 or 704, procedures that require that no contents of any communication originated or sent by a United States person shall be disclosed, disseminated, used or retained for longer than 7 days unless a court order under section 105 is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

***Current definition of "wire communication" deleted.*** Under current law, subsection 101(*l*) defines the term "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." Sec. 9(b)(4) of S. 3931, Sec. 209(b)(4) of S. 3929, would strike this subsection.

***Contents.*** The current definition of "contents" in subsection 101(n) of FISA, 50 U.S.C. § 1801(n),[14] would be replaced with a new definition. Under Sec. 9(b)(5) of S. 3931, Sec. 209(b)(5) of S. 3929, "contents," "when used with respect to a communication, includes any information concerning the substance, symbols, sounds, words, purport, or meaning of a communication, and does not include dialing, routing, addressing, or signaling information."

**Electronic surveillance without a court order to acquire foreign intelligence information pursuant to Attorney General certification.** Section 102 of FISA, 50 U.S.C. § 1802, authorizes electronic surveillance without a court order to acquire foreign intelligence information for up to one year upon certification by the Attorney General in writing under oath that certain criteria have

---

[14] Under the current subsection 101(n) of FISA, "'contents,' when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication."

been met.[15] As amended by Sec. 9(c) of S. 3931, Sec. 209(c) of S. 3929, the application under subsection 102(a)(1)(A)(i) of FISA, 50 U.S.C. § 1802(a)(1)(A)(i), would be expanded to include, among other things, electronic surveillance directed at (not "solely directed at") the acquisition of the contents of communications of 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 an agent of a foreign power other than a United States person, as defined in subsection 101(b)(1) of FISA, 50 U.S.C. § 1801(b)(1).[16] The amendment also deletes a requirement in current Sec. 102(a)(1)(B) of FISA, 50 U.S.C. § 1801(a)(1)(B), that the Attorney General certify that "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a U.S. person is a party."

Under both the current and amended versions of subsection 102(a)(2) of FISA, 50 U.S.C. § 1802(a)(2), an electronic surveillance authorized under subsection 102(a)(1) of FISA, 50 U.S.C. § 1802(a)(1), may only be conducted in accordance with the Attorney General's certification and applicable minimization procedures. Both require the Attorney General to assess compliance with such procedures and to report his assessments to the congressional intelligence committees under subsection 108(a) of FISA, 50 U.S.C. § 1808(a). Under the amended language, if such an electronic surveillance is directed at an agent of a foreign power, the Attorney General's report assessing compliance with the minimization procedures must also include a statement of the facts and circumstances relied upon to justify the belief that the target of the electronic surveillance is an agent of a foreign power.

Under the current and amended subsection 102(a)(3) of FISA, 50 U.S.C. § 1802(a)(3), the Attorney General must immediately transmit under seal to the FISC a copy of the applicable certification, which shall remain under seal unless certain criteria are met.[17]

The current Sec.102(a)(4), 50 U.S.C. § 102(a)(4), permits the Attorney General to direct a specified common carrier to provide any information, facilities, or technical assistance necessary to accomplish an electronic surveillance authorized under subsection 102(a) in a manner which will protect its secrecy and produce a minimum of interference with the services such carrier is providing to its customers, and to maintain any records the carrier wishes to retain concerning such surveillance or the aid furnished with respect thereto under security procedures approved by the

---

[15] Current Sec. 102(a)(1) requires that the Attorney General certify in writing under oath that "the electronic surveillance is solely directed at" the acquisition of the types of information specified. As amended by Sec. 9(c) of S. 3931, Sec. 209(c) of S. 3929, the word "solely" would be deleted.

[16] Current law does not include the acquisition of the contents of communications of agents of foreign powers. Under current law, the contents of communications acquired must be transmitted by means of communications used exclusively between or among such foreign powers.

[17] The only difference between the current criteria and those included in subsection 103(a)(3) of FISA under the two bills here under consideration is the deletion of a reference to section 101(h)(4), which is consistent with the earlier discussed deletion of the current 101(h)(4) and replacement with new language.

Attorney General and the Director of National Security. This provision is absent from the proposed subsection 102(a) of FISA, new 50 U.S.C. § 1802(a).

**Acquisition of foreign intelligence information for up to one year concerning persons outside the United States upon Attorney General certification.** The proposed subsection 102(b)(1) of FISA, Sec. 9(c) of S. 3931, Sec. 209(c) of S. 3929, creates a new authority for the President, acting through the Attorney General, to authorize the acquisition of foreign intelligence information for periods of up to one year concerning a person reasonably believed to be outside the United States if the Attorney General certifies in writing under oath that

> (A) the acquisition does not constitute electronic surveillance as defined in section 101(f);
> (B) the acquisition involves obtaining the foreign intelligence information from or with the assistance of a wire or electronic communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person thereof) who has access to wire or electronic 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;
> (C) a significant purpose of the acquisition is to obtain foreign intelligence information; and
> (D) the minimization procedures to be employed with respect to such acquisition activity meet the definition of minimization procedures under section 101(h).

The certification need not identify the specific facilities, places, premises, or property at which the acquisition will be directed. Compliance with the Attorney General's certification and minimization procedures would be required. The Attorney General is also directed to report his assessments regarding compliance with such procedures to the congressional intelligence committees under subsection 108(a) of FISA, 50 U.S.C. § 1808(a). A copy of the Attorney General's certification would be immediately transmitted to the FISC and there maintained under seal unless it is necessary to determine the legality of the acquisition under proposed subsection 102(o) of FISA.[18]

Under the proposed subsection 102(c) of FISA, with respect to such an acquisition, the Attorney General would be authorized to direct a specified person to furnish the government with all information, facilities, and assistance needed to accomplish the acquisition in a manner that will protect its secrecy and minimize interference with the services that such a person is providing to the target. Any records the person providing aid to the Government wishes to maintain must be kept under security procedures approved by the Attorney General and the Director of National Intelligence (DNI). New subsection 102(d) of FISA would require the government to compensate the specified person furnishing the aid at the prevailing rate.

---

[18] New subsection 102(o) of FISA would permit an aggrieved person against whom evidence obtained or derived from such an acquisition is to be or has been used or disclosed in a federal, state, or local proceeding to move to suppress the evidence on the grounds that the information was unlawfully acquired; or the acquisition was not made in conformity with an order of authorization or approval.

If the person so directed fails to comply with the Attorney General's directive to provide such aid, then, under proposed subsection 102(e) of FISA, the Attorney General could take recourse to the FISC to compel compliance with the directive. Failure to obey the resulting FISC order could be punished as contempt of court.

Under the new subsection 102(f) of FISA, a person receiving such a directive would have a right to challenge the legality of the directive by filing a petition with the petition review pool of FISC judges established under subsection 103(e)(1) of FISA.[19] The petition must be immediately assigned by the FISC Presiding Judge to one of the judges in the pool. Within 24 hours of the assignment of the petition, the assigned judge must conduct an initial review of the directive. If the petition is deemed frivolous, it must be immediately denied and the directive or portion of the directive that is the subject of the petition must be affirmed. If the assigned judge determines that the petition is not frivolous, the assigned judge must consider the petition and make a written statement for the record of his determination and the reasons underlying it for the record within 72 hours. 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 102 or is otherwise unlawful. If the judge does not modify or set aside the directive, he must immediately affirm it and order the recipient's compliance.

A petition to the FIS Court of Review, by the Government or any person receiving such a directive seeking review of an FISC decision to affirm, modify, or set aside the directive must be made within seven days of the issuance of the FISC decision. The FIS Court of Review must provide for the record a written statement of the reasons for its decision. The Government or any person receiving such a directive seeking review of the FIS Court of Review decision may petition the U.S. Supreme Court for a writ of certiorari. The FIS Court of Review must transmit its record under seal to the Supreme Court. Proposed subsection 102(g) of FISA.

Judicial proceedings under Section 102 must be conducted expeditiously, and the record of such proceedings, including petitions filed, orders granted, and statements for 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. Proposed subsection 102(h).

All petitions under this section are to be filed under seal. In proceedings under Section 102 of FISA, upon request by the Government, any Government submissions or portions of submissions, which may contain classified information, may be reviewed by the court ex parte and in camera. Proposed subsection 102(i).

---

[19] Under current subsection 103(e)(1) of FISA, 50 U.S.C. § 1803(e)(1), three FISC judges 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 1861(f)(1) of this title.

**Limitation on liability.** Proposed subsection 102(j) of FISA would preclude any cause of action in any court against any provider of a communication service or other person (including any officer, employee, agent, or other specified person thereof) for furnishing information, facilities, or assistance to the Government pursuant to a directive under new subsections 102(a) or 102(b).

**Use or disclosure of information acquired under Attorney General authorization under Section 102 of FISA.** Under proposed subsection 102(k) of FISA, information regarding a United States person, acquired pursuant to an Attorney General authorization under Section 102 of FISA, 50 U.S.C. § 1802, may be used or disclosed by federal officers and employees without the consent of that United States person, only in accordance with minimization procedures required by either subsection 102(a) or subsection 102(b), as applicable. Information acquired under this section may be used or disclosed by federal officers or employees only for lawful purposes. Under proposed subsection 102(*l*), no information acquired under Section 102 shall be disclosed for law enforcement purposes unless the disclosure is accompanied by a statement that "such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General." New subsection 102(k) also provides that no otherwise privileged communication obtained in accordance with or in violation of Section 102 shall lose its privileged character.

**Procedures for use or disclosure against an aggrieved person in a federal, state, or local proceeding of information obtained or derived from an acquisition under Section 102 of FISA .** Proposed subsections 102(m) and (n) of FISA, respectively, provide procedures for use or disclosure of such information in federal proceedings or in state or local proceedings.

***Use or disclosure in federal proceedings.*** Under Sec. 9(c) of S. 3931, Sec. 209(c) of S. 3929, the federal government may only introduce into evidence or otherwise use or disclose information acquired by or derived from an acquisition under Section 102 of FISA, 50 U.S.C. § 102, in any trial, hearing or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States against an aggrieved person, if it complies with the requirements of proposed subsection 102(m). Under this subsection, the Government, prior to the proceeding or at a reasonable time prior to seeking to place the information in evidence or otherwise to use or disclose the information, must notify the aggrieved person and the court or other authority in which the information is to be used or disclosed of the United States' intent to do so.

***Use or disclosure in state or local proceedings.*** Somewhat similarly, under proposed subsection 102(n), a state or political subdivision may only introduce into evidence or otherwise use or disclose information obtained by or derived from a Section 102 acquisition, in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other state or local authority, against an aggrieved person, if the state or political subdivision notifies the aggrieved person, the court or other authority in which the information is to be used or disclosed, and the U.S. Attorney General, of the state or political subdivision's intent to so use or disclose the information.

***Aggrieved person's motion to suppress.*** An aggrieved person against whom information acquired by or derived from a Section 102 acquisition is intended to be used or disclosed in a federal, state, or local proceeding may move to suppress the evidence so acquired or derived on one of two grounds: the information was unlawfully acquired, or the acquisition was not made in conformity with an order of authorization or approval. A motion to suppress is to be made before the trial, hearing, or other proceeding involved unless there is no opportunity to make such a motion or unless the person is not aware of the grounds of the motion. Proposed subsection 102(o) of FISA.

***Consideration by U.S. district court of the legality of an acquisition upon Attorney General affidavit.*** Under proposed subsection 102(p) of FISA, if the Attorney General files an affidavit under oath, pursuant to proposed subsection 102(b) of FISA, that disclosure or an adversary hearing would harm the national security of the United States; then whenever a court or other authority is given notice under subsections 102(m) or 102(n), a motion to suppress is filed under subsection 102(o), or a request is made by an aggrieved person under any other federal or state statute or rule before a federal or state court or other authority, seeking to discover or obtain an Attorney General directive or other materials related to a Section 102 acquisition, or seeking to discover, obtain, or suppress evidence or information acquired by or derived from a Section 102 acquisition, the U.S. district court before whom the matter is pending, or the U.S. district court in the same district as the other authority before whom the motion is made, shall determine whether the acquisition under Section 102 was lawfully conducted and authorized. The U.S. district court may review in camera and ex parte the Attorney General's directive and other materials related to the Section 102 acquisition necessary to making its determination. The court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the directive or other related materials only where such disclosure is necessary to an accurate determination of the legality of the acquisition.

Under proposed subsection 102(q) of FISA, if the U.S. district court were to find that an acquisition authorized under Section 102 of FISA was not lawfully authorized or conducted, the evidence thereby unlawfully obtained or derived would be suppressed. If the U.S. district court were to determine that the acquisition was lawfully authorized and conducted, the court would deny the aggrieved person's motion except to the extent that due process requires discovery or disclosure. Any orders granting motions or requests under subsection 102(o), decisions holding that a Section 102 authorization was not lawfully authorized or conducted, or U.S. district court orders requiring review or granting disclosure of directives or materials related to a Section 102 acquisition, would be binding on all other federal or state courts except a U.S. court of appeals or the U.S. Supreme Court. Proposed subsection 102(r) of FISA.

**Authority for federal officers who acquire foreign intelligence information under Section 102 of FISA to consult with federal or state law enforcement.** Federal officers who acquire foreign intelligence information pursuant to Section 102 of FISA, 50 U.S.C. § 1802, may consult with federal law enforcement officers or state or local law enforcement personnel to coordinate efforts to investigate or protect against

> (1) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> (2) sabotage, international terrorism, or the development or proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power;
> (3) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

Such coordination would not preclude the certifications required under subsections 102(a) or (b). Proposed subsection 102(t).

**Retention of Directives and Orders.** Under proposed subsection 102(u), directives made under Section 102 of FISA and orders granted under that section must be retained for 10 years.

**Designation of FISC judges.** Under Sec. 9(d) of S. 3931, Sec. 209(d) of S. 3929, Sec. 103(a) of FISA is amended to authorize the Chief Justice of the United States to publicly designate 11 district court judges from *at least* seven of the U.S. judicial circuits to be FISC judges, of whom no fewer than three shall reside within 20 miles of the District of Columbia. A new subsection 103(g) would also be added to FISA providing express authority for applications for an FISC order under Title I of FISA if the President has authorized the Attorney General in writing to approve applications to the FISC. An FISC judge to whom an application is made is explicitly authorized to grant an order under Section 105 of FISA approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information.

**Applications for FISC orders under Sec. 104 of FISA.** Sec. 9(e) of S. 3931, Sec. 209(e) of S. 3929, makes a series of amendments to Sec. 104 of FISA, 50 U.S.C. § 1804. Current subsections 104(a)(6) through (11) are deleted from FISA and replaced by new subsections 104(a)(6) through (10). An application for a court order to authorize electronic surveillance under FISA must contain, among other things, a certification that certain requirements are met. Under current law, such certification or certifications are made 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. As amended, the certification would be made by "the Assistant to the President for National Security Affairs or an executive branch official authorized by the President to conduct electronic surveillance for foreign intelligence purposes."[20]

---

[20] As amended, such official must certify:

> (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 —

(continued...)

Under current law, subsection 104(b) of FISA, 50 U.S.C. § 1804(b) deals with the exclusion of certain information from an application for a FISC order authorizing electronic surveillance where the target is a foreign power as defined in subsection 101(a)(1), (2), or (3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power. In such circumstances, the application currently is required to include a statement as to whether physical entry is required to effect the surveillance, and to contain such information about the surveillance techniques and communications or other information concerning U.S. persons likely to be obtained as may be necessary to assess the proposed minimization procedures. Sec. 9(e)(2) and (3) of S. 3931, Sec. 209(e)(2) and (3) of S. 3929, would strike current Sec. 104(b) of FISA, 50 U.S.C. § 1804(b), and redesignate subsections 104(c)-(e) as 104(b)-(d) of FISA.

Current subsection 104(e)(1)(A) (as redesignated above, subsection 104(d)(1)(A)) provides that, 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 104(a), 50 U.S.C. § 1804(a) an application under that subsection for a target described in section 101(b)(2) of FISA, 50 U.S.C. § 1801(b)(2).[21] New

---

[20] (...continued)

> (i) the information sought is the type of foreign intelligence information designated; and
> (ii) such information cannot reasonably be obtained by normal investigative techniques[.]

With respect to the matters that must be certified by this official, new subsections 104(a)(6)(A)-(C) are the same as current subsections 104(a)(7)(A)-(C). The new language deletes a requirement in current subsection 104(a)(7)(D) that the application include a certification from such an official that designates the type of foreign intelligence information being sought according to the categories described in Sec. 101(e) of FISA. New subsection 104(a)(6)(D) is the same as the current 104(a)(7)(E).

As amended, subsection 104(a)(7) of FISA requires that, an application for a court order authorizing electronic surveillance must include "a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this title should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter." This language is the same as the current subsection 104(a)(10) of FISA, 50 U.S.C. § 1804(a)(10).

New subsection 104(a)(8) requires "a summary description of the nature of the information sought and the type of communications or activities to be subject to the surveillance." Current subsection 104(a)(6) of FISA, 50 U.S.C. § 1804(a)(6) requires "a detailed description" of such information. New subsection 104(a)(9) is similar to current subsection 104(a)(9) of FISA, 50 U.S.C. § 1804(a)(9), except that current law requires "a statement," while the amended language requires "a summary statement." New subsection 104(1)(10) is similar to current subsection 104(a)(8) of FISA, 50 U.S.C. § 1804(a)(8), except that current law requires "a statement," while the new language requires "a summary statement."

[21] Section 101(b)(2) of FISA, 50 U.S.C. § 1801(b)(2), sets out several categories of persons (continued...)

subsection 104(d)(1)(A) would expand this list to include the Director of the Central Intelligence Agency.

**Issuance of FISC order under Sec. 105 of FISA.** Sec. 9(f) of S. 3931, Sec. 209(f) of S. 3929, would amend Sec. 105 of FISA, 50 U.S.C. § 1805, in a number of respects. Current subsection 105(a)(1) provides that, upon an application under Sec. 104 of FISA, the FISC judge shall enter an ex parte order as requested or as modified approving the electronic surveillance in the application if he finds that "the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information." As amended, this subsection would be stricken and subsections 105(a)(2) through (a)(5) of FISA, 50 U.S.C. §§ 1805(a)(2) through (a)(5), would be redesignated subsections 105(a)(1) through (a)(4), 50 U.S.C. §§ 1805(a)(1) through (a)(4).

***Specifications to be included in a FISC order for electronic surveillance.*** Current subsection 105(c)(1) of FISA, 50 U.S.C. § 1805(c)(1), which deals with specifications to be included in an order approving electronic surveillance under Sec. 105 of FISA, would also be deleted and replaced with a new subsection 105(c)(1), which includes in the following order the current subsections 105(c)(1)(A), (B), (E), (C) and (D), and deletes current requirements in subsections 105(c)(1)(F). The latter provision provides that an order approving electronic surveillance under Section 105 of FISA, 50 U.S.C. § 1805, shall specify, "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."

Current subsection 105(d) deals with the exclusion of certain information from applications for court orders authorizing electronic surveillance where the target of the surveillance is a foreign power as defined in Sec. 101(a)(1), (2), or (3), and each facility or place to be surveilled is owned, leased, or exclusively used by that foreign

---

[21] (...continued)
who are defined to be "agents of foreign powers," regardless of whether or not they are United States persons. Under current law, these categories include any person who:

> (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
> (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

power. It also requires description of information sought, the communications to be subject to surveillance, and the type of electronic surveillance involved, including whether physical entry would be required. As amended, the current language would be stricken and replaced with a requirement that, "Each order under this section specify the type of electronic surveillance involved, including whether physical entry is required."

***Extensions of orders for electronic surveillance under FISA.*** Under current Section 105(e)(2), extensions of an order authorizing electronic surveillance under Title I of FISA, 50 U.S.C. § 1801 *et seq*., 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,[22] with two exceptions. First, an extension of an FISC order for a surveillance targeted against a foreign power that is a foreign-based political organization, not substantially composed of United States persons; or an entity that is directed and controlled by a foreign government or governments; or targeted against a group engaged in international terrorism or activities in preparation therefor 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. Second, an extension of an order under FISA 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 one year.

As amended, current subsection 105(e)(2), 50 U.S.C. § 105(e)(2) would be stricken and replaced with a new subsection 105(e)(2), providing that extensions of an order issued under Title I of FISA may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order and may be for a period not longer than the court determines to be reasonable or one year, whichever is less.

***Emergency authorization of electronic surveillance without a court order.*** Current subsection 105(f), 50 U.S.C. § 1805(f), provides for emergency authorization of electronic surveillance without a court order for up to 72 hours by the Attorney General if he reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can, with due diligence, be obtained; and that the factual basis for issuance of an order under this title to approve such surveillance exists. The Attorney General or his designee must notify an FISC judge of the emergency employment of electronic surveillance at the time of its authorization. During this 72 hour window, a court order under Sec. 105 must be sought. Subsection 105(f) also currently requires termination of the

---

[22] Current subsection 105(e)(1) provides generally for electronic surveillance for the period specified in the application or for up to 90 days, whichever is less; for the period specified in the application or for up to 120 days, whichever is less, where the target is an agent of a foreign power who is not a U.S. person; and for the period specified in the application or for up to one year, for foreign power targets who are foreign governments or components thereof; foreign nation or nations or factions thereof, not substantially composed of United States persons; or entities openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments.

surveillance when the information sought is acquired, if a FISC order approving the surveillance is denied, or at the end of the 72 hours, whichever is earliest; and restricts use or disclosure of information acquired or derived from that surveillance if a court order is not obtained.

Under Sec. 9(f)(5) of S. 3931, Sec. 209(f)(5) of S. 3929, the current subsection 105(f) of FISA, 50 U.S.C. § 1805(f) would be deleted and replaced with an new subsection 105(f). While current law authorizes the Attorney General to determine whether to authorize electronic surveillance without a court order on an emergency basis if he reasonably determines that the requisite factors exist, the new language would grant such authority to "an executive branch officer appointed by the President with the advice and consent of the Senate who is authorized by the President to conduct electronic surveillance." The new language would require that the Attorney General be informed of the emergency electronic surveillance. While current law requires a FISC judge to be informed by the Attorney General or his designee at the time of authorization of emergency electronic surveillance, the new law would require such judge to be informed "as soon as practicable following such authorization that the decision has been made to employ emergency electronic surveillance." New subsections 105(f)(2)(a) and (b).

Current law requires that an application for an FISC order authorizing electronic surveillance be made to the FISC judge so notified within 72 hours of the authorization of employment of emergency electronic surveillance. Under the new provision, an application must be made to that FISC judge or another FISC judge as soon as possible within seven days after the surveillance is authorized. Under current subsection 105(f), in the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information is obtained, when the application for the order is denied, or after the expiration of 72 hours from the time when the Attorney General approved the emergency electronic surveillance, whichever is earliest. As amended, the period of 72 hours after the Attorney General approved the emergency electronic surveillance would be replaced by one of seven days after approval of the emergency electronic surveillance by an executive branch officer appointed by the President with the advice and consent of the Senate who is authorized by the President to conduct electronic surveillance. The restrictions on disclosure and use of information obtained or derived from such an emergency electronic surveillance in the absence of an authorizing court order parallel those in existing law. While, under current law, if the Attorney General authorizes such emergency employment of electronic surveillance, he shall require that the minimization procedures required by this subchapter for the issuance of a judicial order be followed, the revised language would provide that, "The official authorizing the emergency employment of electronic surveillance shall require that the minimization procedures required by this title for issuance of a court order be followed." New subsection 105(f)(1)(D) of FISA.

***Limitations of liability for providers aiding in a FISA electronic surveillance or physical search.*** Sec. 9(f) of S. 3931, Sec. 209(f) of S. 3929, would also modify subsection 105(i) dealing with limitations of liability for those who provide information, facilities, or technical assistance with respect to execution of a FISA electronic surveillance or physical search. As amended, no cause of action would lie against any provider of electronic communication service, landlord,

custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any such aid in accordance with a court order or a request for emergency assistance under this title for electronic surveillance or physical search, or 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 as defined in Sec. 101(f) of FISA.

**Use of information acquired by electronic surveillance under FISA.** Sec. 106 of FISA limits the use by federal, state, or local governments of information regarding unconsenting U.S. persons acquired or derived from electronic surveillance under FISA. It also includes notification requirements and provides an opportunity for an aggrieved person against whom such information is proffered in an official proceeding to move to suppress such information if it was unlawfully acquired or if the surveillance was not made in conformity with an order of authorization or approval.

Under Sec. 9(g) of S. 3931, Sec. 209(g) of S. 3929, Sec. 106(i) of FISA, 50 U.S.C. § 1806(i), which deals with destruction of unintentionally acquired information, would be modified to provide that, where *any communication* is unintentionally acquired by an electronic, mechanical, or other surveillance device, in 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 in the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person. Current subsection 106(i) includes parallel provisions, but applies only to unintentionally acquired *radio* communications. (Emphasis added.)

The import of a second amendment to subsection 106(i) of FISA, 50 U.S.C. § 1806(i), in Sec. 209(g)(1)(B) of S. 3886, Sec. 9(g)(1)(B) of S. 2453, is somewhat unclear. The provision indicates that subsection 106(i) of FISA would be amended by "inserting 'contain significant foreign intelligence information or' after 'Attorney General determines that the contents' inserting 'contain significant foreign intelligence information or.'" [sic] As written, this language is unclear. If one were to insert "contain significant foreign intelligence information or contain significant foreign intelligence information or" after "Attorney General determines that the contents," the result would be an amended provision reading:

> In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, 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.

This would expand the circumstances in which destruction of the unintentionally acquired contents of the communication would be forestalled. However, the inclusion twice in the amending language of the phrase "inserting 'contain foreign

intelligence information or'" suggests that one of these inclusions may be redundant.[23]

Sec. 9(g)(2) of S. 3930, Sec. 209(g)(2) of S. 3929, makes a conforming amendment to subsection 106(k), replacing "104(a)(7)" with "104(a)(6)," reflecting a change made to Sec. 104 of FISA, 50 U.S.C. § 1804, by Sec. 9(e) of S. 3930, Sec. 209(e) of S. 3929.

**Congressional oversight under Sec. 108 of FISA regarding a document management system for applications for FISC orders authorizing electronic surveillance.** Sec. 9(h) of S. 3931, Sec. 209(h) of S. 3929, amends the congressional oversight provisions of Sec. 108 of FISA, 50 U.S.C. § 1808, to add a new subsection 108(c) requiring the Attorney General and the Director of National Intelligence, in consultation with the Director of the FBI, the Director of the NSA, the Director of the CIA, and the FISC, to conduct a feasibility study to develop and implement a secure, classified document management system that would permit prompt preparation, modification, and review by appropriate personnel of the Department of Justice, the FBI, the NSA, and other applicable U.S. government elements, of applications for FISC orders authorizing electronic surveillance before their submittal to the FISC. Such a system would permit and facilitate prompt submittal of applications and all other matters, including electronic filings to the FISC under Sections 104 or 105(g)(5)[24] of FISA, and would permit and facilitate the prompt transmittal of FISC rulings to personnel submitting such applications.

**Amendments to FISA, Title I, Relating to Weapons of Mass Destruction.** Sec. 9(i) of S. 3931, Sec. 209(i) of S. 3929, made a series of amendments to Title I of FISA, which deals with electronic surveillance.

***Agent of a Foreign Power definition.*** Section 101(b)(1) of FISA, 50 U.S.C. § 1801(b)(1), lists a number of categories of persons, other than U.S. persons, who are defined as "agents of a foreign power" under FISA. Sec. 9(i)(1) of S. 3931, Sec. 209(i)(1) of S. 3929, would add a new subsection 101(b)(1)(E) to the definition of "agent of a foreign power" under subsection 101(b)(1), and redesignate current subsection 101(b)(1)(E) of FISA as subsection 101(b)(1)(F). Under the new definitional category, any person other than a U.S. person who "engages in the

---

[23] It would seem that the same impact upon subsection 106(i) might be achieved by the deletion of either of the two iterations of the phrase. Thus, the amendment might be phrased: Section 106 is amended in subsection (i) by "inserting 'contain significant foreign intelligence information or' after 'Attorney General determines that the contents.'" Alternatively, the amendment might state: Section 106 is amended, "after 'Attorney General determines that the contents' by inserting 'contain significant foreign intelligence information or.'"

[24] There is no current Sec. 105(g)(5) of FISA. Sec. 105(g) of FISA, 50 U.S.C. § 1805(g) deals with "testing of electronic equipment; discovering unauthorized electronic surveillance; training of intelligence personnel."

development or proliferation of weapons of mass destruction, or activities in preparation therefor" would be deemed an "agent of a foreign power" under FISA.

Section 101(b)(2) of FISA, 50 U.S.C. § 1801(b)(2) lists a series of categories of persons (whether or not they are U.S. persons) who are also defined as "agents of a foreign power." Under current subsection 101(b)(2)(C), any person who "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power" is deemed to be an "agent of a foreign power." As amended by Sec. 9(i)(1)(B) of S. 3931, Sec. 209(i)(1)(B) of S. 3929, under subsection 101(b)(2)(C) of FISA, 50 U.S.C. § 1801(b)(2)(C), any person who "knowingly engages in sabotage, international terrorism, or the development or proliferation of weapons of mass destruction or activities that are in preparation therefor, for or on behalf of a foreign power" would be considered an "agent of a foreign power" under FISA.

***New definition of Weapon of Mass Destruction.*** Sec. 9(i)(1)(C) of S. 3931, Sec. 209(i)(1)(C) of S. 3929, would add a new subsection 101(*l*) to the definitions in Section 101 of FISA, 50 U.S.C. § 1801. Under this new subsection, "weapon of mass destruction" would mean:

> (1) any destructive device (as that term is defined in section 921 of title 18, United States Code) that is intended or has the capability, to cause death or serious bodily injury to a significant number of people;
> (2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors;
> (3) any weapon involving a biological agent, toxin, or vector (as those terms are defined in section 178 of title 18, United States Code); or
> (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.

Sections 101(e)(1)(B),[25] 106(k)(1)(B),[26] and 305(k)(1)(B)[27] of FISA, 50 U.S.C. §§ 1801(e)(1)(B), 1806(k)(1)(B), and 1825(k)(1)(B), each would be amended to encompass not only sabotage or international terrorism, but also the development or proliferation of weapons of mass destruction.

**Conforming Amendments to Titles I and III of FISA to Accommodate International Movements of Targets.** Sec. 9(j) of S. 3931, Sec. 209(j) of S. 3929, amends both Sections 105(e) and 304(d) of FISA, 50 U.S.C. §§ 1805(e) and 1824(d), dealing with the duration and extension of FISC orders authorizing electronic surveillance and physical searches, respectively under FISA, to address international movements of targets. A new subsection 105(e)(4) would be added to FISA, providing, "An order issued under this section shall remain in force during the

---

[25] As amended, Section 101(e)(1)(B) of FISA, 50 U.S.C. § 1801(e)(1)(B), would define "foreign intelligence information," to include, among other things, "sabotage, international terrorism, or the development or proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power."

[26] As amended, Section 106(k)(1)(B) of FISA, which deals with consultation with federal law enforcement officers or state or local law enforcement personnel by those who engage in electronic surveillance to acquire foreign intelligence information under FISA, would permit:

> (1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision) to coordinate efforts to investigate or protect against
> . . .
> (B) sabotage, international terrorism, or the development or proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power;
> . . .
> . . . .

[27] As amended, Section 305(k)(1)(B) of FISA, which deals with consultation with federal law enforcement officers or state, or local law enforcement personnel by those who engage in physical searches to acquire foreign intelligence information under FISA, would permit:

> (1) Federal officers who conduct physical searches to acquire foreign intelligence information under this subchapter may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision) to coordinate efforts to investigate or protect against
>
> . . .
> (B) sabotage, international terrorism, or the development or proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power;
> . . .
> . . . .

authorized period of surveillance notwithstanding the absence of the target from the United States, unless the Government files a motion to extinguish the order and the court grants the motion." Similarly, a new subsection 304(d)(4) would be added to FISA, stating, "An order issued under this section shall remain in force during the authorized period of physical search notwithstanding the absence of the target from the United States, unless the Government files a motion to extinguish the order and the court grants the motion."

## Conforming Amendment to Table of Contents of FISA

Sec. 10 of S. 3931, Sec. 210 of S. 3929, would make conforming amendments to the table of contents of FISA, to reflect the replacement of the current Section 102 of FISA with a new Section 102; the repeal of the wartime authorities under FISA, Sections 111, 309, and 404; and the creation of a new Title VII of FISA and redesignation of the current Title VII as Title VIII of FISA.