Order Code RS22140
May 9, 2005

The SAFE Acts of 2005: H.R. 1526 and S. 737 — A Sketch

Charles Doyle
Senior Specialist
American Law Division

Summary

Somewhat different SAFE Acts have been introduced in both the House and Senate: S. 737, the Security and Freedom Enhancement Act of 2005 (introduced by Senator Craig) and H.R. 1526, the Security and Freedom Ensured Act of 2005 (introduced by Representative Otter). Although the Senate bill is more detailed, they address many of the same issues, most of which relate to the USA PATRIOT Act — roving Foreign Intelligence Surveillance Act (FISA) wiretaps, delayed notification of "sneak and peek" search warrants, library and similar exemptions from FISA tangible item orders and communications related to national security letters, the definition of "domestic terrorism," and expansion of the sunset provisions of the USA PATRIOT Act.

This report is an abridged version — without footnotes and citations — of CRS Report RL32907, *Security and Freedom Ensured Act of 2005 (SAFE Act)(H.R. 1526) and Security and Freedom Enhancement Act of 2005 (SAFE Act)(S. 737): Section by Section Analysis*.

Section 1. *Short Title*: Section 1 of the bills contains their short titles, the "Security and Freedom Ensured Act of 2005 (SAFE) Act" in the case of H.R. 1526; and "Security and Freedom Enhancement Act of 2005" or "SAFE Act" in the case of S. 737.

Section 2. *Limitation on Roving Wiretaps Under Foreign Intelligence Surveillance Act of 1978*: The Foreign Intelligence Surveillance Act (FISA) permits federal judges assigned to serve on the Foreign Intelligence Surveillance Court to issue orders authorizing, for foreign intelligence gathering purposes, electronic surveillance; physical searches; the use of trap and trace devices and pen registers; and access to tangible items.

Subsection 1805(c) of FISA describes the specifications and directions for FISA electronic surveillance orders. Before 9/11, FISA electronic surveillance orders specified (1) the identity, *if known*, or the description of the target of the surveillance, (2) the nature and location of the facilities or places at which the surveillance was directed, and (3) if

requested, the identity of communications providers, landlords and other person whose assistance would facilitate execution of the order.

Section 206 of the USA PATRIOT Act temporarily altered this third feature to permit a general command for third party assistance without identifying a specific person, if the target of the order regularly changed telephones or meeting places or took other evasive steps in order to thwart surveillance efforts. The intelligence authorization act for 2002 altered the second feature to require identification of the nature and location of targeted facilities and places only if they were known. Thus, at least temporarily, FISA surveillance orders may be issued that simply describe the target but do not otherwise identify the target, the facilities or places to be targeted, or those communications providers or others whose assistance will be commanded to facilitate execution of the order.

Both the House and Senate bills amend subsection 1805(c) to require that FISA surveillance orders identify either the target or the facilities or places targeted; orders merely describing the target because the target's identity is unknown must identify the facilities or places targeted and orders that do not identify the facilities or places because they are unknown must identify the target. If the facilities or places cannot be identified in the order, both bills limit execution of a FISA surveillance order to times when the target is present at the facility or place under surveillance.

Section 3. *Limitations on Delayed Notice Search Warrants - In General*: The Fourth Amendment to the United States Constitution prohibits unreasonable searches and seizures, U.S. Const. Amend. IV. The amendment does not apply when there is no reasonable expectation of privacy with respect to the item seized, such as information or other property in the possession of a third party for example. Yet where a reasonable expectation of privacy exists and subject to certain exigent circumstances, the Fourth Amendment requires officers executing a search warrant to knock and announce their purpose before entering to execute the warrant. Prior to the USA PATRIOT Act, the Federal Rules of Criminal Procedure which implement the amendment, instructed officers to leave a notice of the search and an inventory of any items seized at the location where the search occurred. The lower federal appellate courts were divided over whether failure to provide notification should be treated as a violation of the rule or as a constitutional violation; and they likewise could not agree on how long notification might be postponed when exigent circumstances justified delayed notification.

Federal law permits delayed notification to customers of government access to their communications stored with service providers — a situation under which there may well be no judicially recognized reasonable expectation of privacy. The law limits delays to instances where contemporaneous disclosure would have adverse consequences. The list of adverse consequences includes factors traditionally recognized as exigent circumstances for Fourth Amendment purposes (risk of injury or flight, of the destruction of evidence, or of the intimidation of a potential witness) and two factors which probably would not be thought to constitute exigent circumstances (seriously jeopardize an investigation or unduly delay a trial). Section 213 of the USA PATRIOT Act amends 18 U.S.C. 3103a to permit delayed notification of the execution of search warrant or court order for a reasonable time in presence of any of the adverse conditions listed in 18 U.S.C. 2705.

The two bills amend subsection 3103a(b) first to limit the grounds justifying delay to those that can be considered exigent circumstances (injury, flight, destruction of evidence, witness intimidation risks) and second to confine the period of delay to no more than 7 days (with the possibility of 21-day extensions).

B. Reports: The bills direct the Attorney General to issue a public report every six months documenting the number of notify postponements and extensions requested and granted or denied, proposed 18 U.S.C. 3103a(c). The Senate bill also insists that the report identify the nature of the crimes that have given rise to subsection 3103a(b) requests.

Section 4. *Privacy Protections for Library, Bookseller, and Other Personal Records Under Foreign Intelligence Surveillance Act of 1978 - In General*: Before the USA PATRIOT Act, FISA authorized judges and magistrates of the FISA court to issue orders affording the Federal Bureau of Investigation (FBI) access to certain business records during the course of gathering foreign intelligence information or investigating international terrorism. Applications were to include "specific and articulable facts" for a belief that the subject of the business records was a foreign power or the agent of a foreign power. The orders could be addressed to any transportation common carrier, public accommodation provider, storage facility or vehicle rental business, and recipients could not disclose them except to the extent necessary to provide access to the records.

Section 215 of the USA PATRIOT Act temporarily rewrote this portion of FISA. In the form scheduled to sunset on December 31, 2005, FISA court orders are available for FBI access to "any tangible things (including books, records, papers, documents, and other items)" without regard to whether they pertain to a foreign power or any of its agents as long as access is sought to obtain foreign intelligence information (not concerning a United States person) or to protect against international terrorism or clandestine intelligence activities. Section 215 kept the nondisclosure feature and granted recipients protection from civil liability for compliance with a FISA order.

Both bills restrict the temporary FISA tangible things access orders to instances where there are specific and articulable reasons to believe that the records pertain to a foreign power or one or more of its agents. The Senate bill alone provides that the order may be no more sweeping than a grand jury subpoena duces tecum issued in the context of an espionage or international terrorism investigation (i.e., it must yield to federally recognized privileges and may not be unreasonable or oppressive). The Senate bill also calls for the order to include notice of the recipient rights that the bill provides.

B. Oversight: Both bills add the House and Senate Judiciary Committees to the Congressional authorities that the Attorney General must keep apprised of the extent of the FBI's use of the FISA access order authority, 50 U.S.C. 1862.

C. Amendments Unique to S. 737: The Senate bill adds: (1) exceptions and 180 day time limits to the nondisclosure feature (with the possibility of 180 day extensions), (2) a procedure to allow a recipient to quash or modify an order, and (3) use provisions comparable to those that apply to the use of information generated by FISA surveillance and physical search orders, proposed 50 U.S.C. 1861(d), (f), (g). H.R. 1526 has no comparable provisions.

Section 5. (*H.R. 1526: Privacy Protections for Computer Users at Libraries Under National Security Authority/ S. 737: Procedural Protections for National Security Letters) - In General*: Four statutes vest federal intelligence officials with the power to demand production of certain information directly rather than invoke the power of a FISA court judge to secure access. These national security letter statutes are (1) 18 U.S.C. 2709 (FBI request to wire or electronic communications service providers for customer name, address, length of service, and local and long distance toll billing records); (2) 12 U.S.C. 3414 (FBI request to financial institutions for records relating to customer transactions); (3) 15 U.S.C. 1681u (FBI request to consumer reporting agencies for consumer name, address, former address, places of employment, former places of employment, and names and addresses of financial institutions with whom a customer has an account); and (4) 15 U.S.C. 1681v (government agency request to consumer reporting agencies for consumer and all other information in the agency's files).

Although they vary somewhat, these statutes generally have no explicit enforcement mechanism nor any means for a recipient to have a request modified or set aside, bar disclosure by recipients of the requests, and have no uniform provisions concerning use of the information provided in response to the request. Section 505 of the USA PATRIOT Act amended three of the four provisions (18 U.S.C. 2709, 12 U.S.C. 3414, 15 U.S.C. 1681u) and section 358 created the fourth (18 U.S.C. 1681v). Each of the amendments (1) made it clear that the request did not have to come from FBI headquarters but could be issued by any of the agents in charge of the various FBI field offices; (2) substituted a relevancy issuance standard for the earlier reason to believe standard; (3) dropped the requirement that the records sought pertain to a foreign power or its agents; and (4) asserted that access could not be sought in connection with an investigation based solely on an American's exercise of his First Amendment rights. In a case now on appeal, one federal district court found that the manner of exercising the national security letter authority under 18 U.S.C. 2709 violated both the Fourth and the First Amendments, the Fourth because of the want of judicial supervision or review and the First because of the facially all encompassing, permanent form of the gag order.

H.R. 1526: The bills treat the national security letter statutes differently. H.R. 1526 simply exempts libraries from the coverage of 18 U.S.C. 2709. Later in the bill, it adds section 505 of the USA PATRIOT Act with its amendments to the national security letter statutes (18 U.S.C. 2709, 12 U.S.C. 3414, and 15 U.S.C. 1681u) to the list of USA PATRIOT Act provisions that expire on December 31, 2005.

S. 737: The Senate makes no such addition to the list of terminating sections nor does it exempt libraries per se from any of national security letter statutes. Instead it rewrites each of the statutes in much the same way it rewrites the FISA access order provisions. Within each of the national security letter statutes, it (1) reestablishes the demand that the information sought be based on specific and articulable facts that suggest that the information sought pertains to a foreign power or one or more of its agents; (2) sets a 90 day time limit for the gag orders based on exigent circumstances (with the possibility of 180 day extensions available from the court on the same basis); (3) permits recipients to challenge both the request and gag orders in court; (4) holds the letters to same standards that apply to grand jury subpoenas duces tecum issued in espionage or international terrorism cases (i.e., they must yield to federally recognized privileges and may not be unreasonable or oppressive); (5) explicitly permits disclosure to those

necessary to comply with the request and to the recipient's attorney; and (6) establishes a procedure for use and suppression of evidence generated by the letters.

Section 6. *Modification of Definition of Domestic Terrorism (H.R. 1526; Section 7 in S. 737)*: Federal law employs two terrorism-related definitions fairly extensively. The first defines "federal crimes of terrorism" by listing a series of specific federal offenses likely to be committed for terrorist purposes, 18 U.S.C. 2332b(g)(5)(text is appended). The second defines "domestic terrorism" generically rather than by reference to any specific federal crime, 18 U.S.C. 2331(5):

> As used in this chapter . . . (5) the term "domestic terrorism" means activities that — (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended — (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States.

Neither domestic terrorism or a federal crime of terrorism is a separate crime. They are used for purposes of cross reference. Thus for example, a federal crime of terrorism as defined in 18 U.S.C. 2332b(g)(5)(B) that involves the risk of serious injury to another person is not subject to the usual statute of limitations and may be prosecuted at any time. Similarly, property derived from and used to facilitate international or domestic terrorism as defined by 18 U.S.C. 2331 is subject to confiscations.

Both bills amend 18 U.S.C. 2331(5) so as to merge the two definitions, "As used in this chapter . . . (5) the term 'domestic terrorism' means activities that — (A) involve acts dangerous to human life that constitute a Federal crime of terrorism (as that term is defined in section 2332b(g)(5) of this title); and (B) occur primarily within the territorial jurisdiction of the United States." H.R. 1526 contains an additional provision that emphasizes that nothing in section 2331 should be construed to preclude enforcement of state terrorism laws; S. 737 has no comparable provision.

Section 6. *(S. 737 only) Privacy Protections for Pen Registers and Trap and Trace Devices - In General*: Trap and trace devices and pen registers are essentially surreptitious "caller id" devices that track the source and destination of incoming and outgoing telephone calls to and from a particular telephone. The Supreme Court has held that their use does not offend any Fourth Amendment protected expectation of privacy. Federal law contains procedures under which authorities may secure judicial approval for the installation and use of trap and trace devices and pen registers in both a law enforcement and an intelligence gathering (FISA) context.

Section 216 and 214 of the USA PATRIOT Act amended the law enforcement and FISA procedures to apply to e-mail and other forms of Internet and electronic communications. The law enforcement amendment requires a report to the issuing court on the specifics on the use of the devices in connection with an Internet communication. The FISA amendment precludes use of the authority in connection with an investigation predicated solely on the exercise of an American target's First Amendment rights. The FISA amendment expires on December 31, 2005; the law enforcement amendment does not.

H.R. 1526: Section 7 of the House bill adds section 216, the law enforcement amendment, to the list of USA PATRIOT Act sections that expire on December 31, 2005.

S. 737: The Senate bill amends both the FISA and the law enforcement procedure to require applicants to include a statement of the specific and articulable facts that give rise to their belief that installation and use of the devices will produce evidence relevant to a criminal investigation. It expands the annual law enforcement reporting requirement to include more specific information concerning the use of the devices and directs that report be made publicly. And it establishes a new notice provision in the law enforcement procedure for the benefit of those interests are implicated by use of the device.

Section 7. *(H.R. 1526 only) Extension of Patriot Sunset Provision - A. In General*: Section 224 of the USA PATRIOT Act creates an expiration date (December 31, 2005) for the sections found in Title II of the act, but exempts from termination several including sections 213 (delayed notification of the execution of search warrant (sneak and peek warrants)), 216 (use of trap and trace devices and pen registers for law enforcement purpose), 219 (nation-wide service of terrorism search warrants). H.R. 1526 removes the exemption for these three sections so that they too expire on December 31, 2005. It also marks section 505 (national security letter amendments) for expiration at that time.

Although it has no similar provision, S. 737 addresses many of the same concerns, as noted earlier, in section 3 (relating to section 213 and limiting the justifications of delayed notification to exigent circumstances and establishing 7-day and 21-day caps for the initial period of delay and any subsequent extensions); in section 6 (relating to section 216 and providing for participant notice in law enforcement trap and trace device and pen register cases; public reports on use of the authority; and presentation of the facts giving specific and articulable justification for the orders); and in section 5 (relating to section 505 and providing for general adjustments in the national security letter statutes).

Boundless Terrorist Search Warrants: In most instances federal judges may only issue search warrants to be executed in their own judicial districts, but in cases of international or domestic terrorism section 219 of the USA PATRIOT Act allows judges in any district where related activities have occurred to issue search warrants that may be executed within or outside the district. Under H.R. 1526, section 219 expires on December 31, 2005.

Section 8. *(S. 737 only) Public Reporting of the Foreign Intelligence Surveillance Act of 1978*: The intelligence reform legislation passed at the end of the 108th Congress, amended FISA directing the Attorney General to report — in a manner consistent with the protection of national security — to the Congressional Judiciary and Intelligence Committee semi-annually on the extent of FISA use, interpretation of the act by the FISA court, and copies of the FISA court opinions, 50 U.S.C. 1871.

S. 737 amends section 1871 to require that the reports be made public, confines the instruction that the report be made in a manner consistent with the protection of national security to information relating to FISA court opinions, but permits the Attorney General to redact for the protection of national security portions of the publicly released opinions. H.R. 1526 has no comparable provisions.