Amendments to the Foreign Intelligence Surveillance Act Set to Expire in 2009

Edward C. Liu
Legislative Attorney

January 6, 2009

Congressional Research Service
7-5700
www.crs.gov
R40138

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

Several recent amendments to the Foreign Intelligence Surveillance Act (FISA) will sunset on December 31, 2009.

Section 6001(a) of the Intelligence Reform and Terrorism Protection Act (IRTPA), also known as the "lone wolf" provision, changed the rules regarding the types of individuals that could be targets of FISA-authorized searches. It permits surveillance of non-U.S. persons engaged in international terrorism, without requiring evidence linking those persons to an identifiable foreign power or terrorist organization.

Section 206 of the USA PATRIOT ACT amended FISA to permit multipoint, or "roving," wiretaps by adding flexibility to the degree of specificity with which the location or facility subject to electronic surveillance under FISA must be identified.

Section 215 of the USA PATRIOT ACT enlarged the scope of documents that could be sought under FISA, and lowered the standard required before a court order could be issued compelling the production of documents.

While these provisions will cease to be prospectively effective on December 31, 2009, a grandfather clause permits them to remain effective with respect to investigations that began, or potential offenses that took place, before the sunset date.

Contents

Contacts

Overview

The Foreign Intelligence Surveillance Act (FISA) provides a statutory framework for government agencies to seek judicially issued warrants from a specialized Foreign Intelligence Surveillance Court (FISC) authorizing the collection of foreign intelligence information via electronic surveillance[1] or physical searches.[2] FISA also provides procedures governing the use of pen registers and trap and trace devices,[3] and for obtaining access to certain business records for foreign intelligence collection.[4] The extent to which the Fourth Amendment's protections are applicable to the government's collection of foreign intelligence is unclear.[5] But, FISA's statutory requirements arguably provide a minimum standard that must be met before foreign intelligence searches or surveillance may be conducted by the government.[6]

A substantial purpose of a FISA warrant must be the collection of foreign intelligence information.[7] Therefore, the procedures for obtaining a warrant under FISA differ from the procedures used in the criminal law enforcement context. While both FISA warrants and criminal warrants incorporate impartial judicial review to determine if probable cause exists, the propositions that must be supported by probable cause are substantially different in either case. In the case of a FISA warrant, the FISC must find probable cause to believe both (1) that the person targeted by the warrant is a foreign power or its agent, and (2) that the subject of the search (*i.e.* the telecommunications or place to be searched) will be used by the target.[8]

Three relatively recent amendments to FISA will expire on December 31, 2009. These provisions are

[1] 50 U.S.C. §§ 1801-1808 (2008).

[2] 50 U.S.C. §§ 1822-1826 (2008).

[3] 50 U.S.C. §§ 1841-1846 (2008). Pen registers capture the numbers dialed on a telephone line; trap and trace devices identify the originating number of a call on a particular phone line. *See* 18 U.S.C. § 3127(3)-(4) (2008).

[4] 50 U.S.C. §§ 1861-1862 (2008).

[5] The Supreme Court has held that the Fourth Amendment's warrant requirement applies in instances of domestic security surveillance. *U.S. v. U.S. District Court*, 407 U.S. 297, 323-4 (1972) (also referred to as the *Keith* case, so named for the District Court judge that initially ordered disclosure of unlawful warrantless electronic surveillance to the defendants). *See, also*, CRS Report WD00002, *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information*, by Elizabeth B. Bazan and Jennifer K. Elsea, at 9-12 (discussing courts' differing application of the Fourth Amendment to searches for the purpose of foreign intelligence collection).

[6] *But*, s*ee* CRS Report WD00002, *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information*, by Elizabeth B. Bazan and Jennifer K. Elsea, at 29-33 ("While the congressional intent to cabin the President's exercise of any inherent constitutional authority to engage in foreign intelligence electronic surveillance may be clear from the exclusivity provision in FISA and from the legislative history of the measure, some support may be drawn from the Court of Review's decision in *In re Sealed Case* for the position that the President continues to have the power to authorize warrantless electronic surveillance to gather foreign intelligence outside the FISA framework").

[7] *See, e.g.*, 50 U.S.C. § 1804(a)(7)(B) (2008). Prior to 2001, the statute had required that "the purpose" of a FISA warrant be foreign intelligence collection.

[8] 50 U.S.C. § 1805(a)(3) (2008). In contrast, federal criminal search warrants require probable cause to believe that instrumentalities, evidence, or fruits of a crime will be found in the place to be searched. *See* Fed. R. Crim. P. 41(c). Criminal warrants authorizing electronic surveillance additionally require probable cause to believe that the target is engaged in criminal activities, that normal investigative techniques are insufficient, and that the facilities that are the subject of surveillance will be used by the target. 18 U.S.C. § 2518(3) (2008).

- Section 6001(a) of the Intelligence Reform and Terrorism Protection Act (IRTPA), also known as the "lone wolf" provision, which simplified the evidentiary showing needed to obtain a FISA warrant to target individuals, other than U.S. citizens or permanent residents, engaged in international terrorism; [9]
- Section 206 of the USA PATRIOT Act, which permitted multipoint, or "roving," wiretaps in certain circumstances by adding flexibility to the manner in which the subject of a FISA warrant is specified;[10] and
- Section 215 of the PATRIOT Act, which broadened the types of records that could be made accessible to the government under FISA.[11]

This report will discuss the state of the law prior to enactment of these provisions, the changes wrought by each of these provisions, and the expected state of the law after the pending sunset date.

"Lone Wolf" Terrorists

Commonly referred to as the "lone wolf" provision, § 6001(a) of IRTPA simplified the evidentiary standard used to determine whether an individual, other than a citizen or a permanent resident of the U.S., who was engaged in international terrorism, could be the target of a FISA warrant. This provision did not modify other standards used to determine the secondary question of whether the electronic surveillance or a physical search of the subject of a warrant is justified in specific situation.

Historical Context

The historical impetus behind enactment of the "lone wolf" provision came to light shortly after the terrorist attacks of September 11, 2001. During the examination of the events leading up to those attacks, it was reported that investigations into one of the individuals believed to be responsible for those attacks had been potentially hampered by the legal requirements governing FISA.[12] Specifically, Federal Bureau of Investigations (FBI) agents investigating Zacarias Moussaoui suspected him of planning a terrorist attack involving piloting commercial airliners, and had detained him in October of 2001 based on a violation of immigration law.[13] The FBI agents had then sought a search warrant under FISA to examine the contents of Moussaoui's laptop computer.[14] But, the agency apparently concluded that it had insufficient information at that time to demonstrate that Moussaoui was an agent of a foreign power, as required by FISA.[15]

[9] P.L. 108-458, § 6001(a).

[10] P.L. 107-56, § 206, *codified at* 50 U.S.C. § 1805(c)(2)(B) (2008).

[11] P.L. 107-56, § 215, *codified at* 50 U.S.C. §§ 1861-2 (2008).

[12] NAT'L COMM. ON TERRORIST ATTACKS UPON THE U.S., *The 9/11 Commission Report*, at 273-274 [hereinafter "*9/11 Comm'n Rep.*"]

[13] *Id.* at 273. Moussaoui, a French national, was present in the United States with an expired visa.

[14] *Id.* at 273-274.

[15] *Id.* at 274. Based upon this conclusion, the FBI "declined to submit a FISA application" to the FISC.

FISA, as it then existed, would have authorized, among other things, physical searches of a laptop if probable cause existed to believe the laptop was owned or used by a foreign power or its agent.[16] The definition of a "foreign power" included "groups engaged in international terrorism or activities in preparation therefor."[17] Individuals involved in international terrorism for or on behalf of those groups were considered "agents of a foreign power."[18] In the weeks leading up to the attacks, it appears that the FBI encountered an actual or perceived insufficiency of information demonstrating probable cause to believe that Moussaoui was acting for or on behalf of an identifiable group engaged in international terrorism.[19]

Legislative Responses

Following these revelations, a number of legislative proposals were put forth to amend the definition of "agents of a foreign power" under FISA so that individuals engaged in international terrorism did not need to be linked to a specific foreign power.[20] These amendments were ultimately enacted with passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).[21] This "lone wolf" provision provides that persons, other than citizens or permanent residents of the U.S., that are engaged in international terrorism are presumptively considered agents of a foreign power.[22] Enactment of this provision obviated any need to provide an evidentiary connection between that individual and a foreign government or terrorist group.

Critics of the "lone wolf" provision argued that the laptop in the Moussaoui case could have been lawfully searched under FISA or the laws governing generic criminal warrants.[23] Critics also expressed concern that the simplified "lone wolf" standard would lead to "FISA serving as a substitute for some of our most important criminal laws."[24]

On the other hand, proponents of the "lone wolf" provision note that the increased self-organization among terror networks has made proving connections to identifiable groups more difficult, and that a "lone wolf" provision is necessary to combat terrorists who use a modern organizational structure.[25]

[16] 50 U.S.C. § 1821-1824 (2001).

[17] 50 U.S.C. § 1801(a)(4) (2001). At the time, foreign powers also included foreign governments, entities controlled by those governments, and factions of foreign nations and foreign-based political organizations that are not substantially composed of United States persons. *Id.* at § (a)(1-6)

[18] 50 U.S.C. § 1801(b)(2)(C) (2001).

[19] *See 9/11 Comm'n Rep.* at 274. It is unclear whether a search of Moussaoui's laptop before September 11, 2001, would have provided enough information to prevent or minimize those attacks.

[20] S. 2586, 107th Cong. (2002); S. 113, 108th Cong. (2003).

[21] P.L. 108-458, § 6001(a).

[22] 50 U.S.C. § 1801(b)(1)(3) (2008).

[23] *See* S.Rept. 108-40 at 33-41 (additional views of Sen. Leahy and Sen. Feingold on a similar "lone wolf" provision in S. 113).

[24] *Id.* at 73 (additional views of Sen. Feingold).

[25] S.Rept. 108-40 at 4-6.

Sunset

The "lone wolf" provision was originally scheduled to sunset on December 31, 2005.[26] However, § 103 of the USA PATRIOT Improvement and Reauthorization Act of 2005 extended the sunset date of the "lone wolf" provision until December 31, 2009.[27] The original sunset provision also included a grandfather clause which allowed it to continue to be effective with respect to investigations that began, or potential offenses that took place, before the provision's sunset date.[28] For example, if an individual is engaged in international terrorism on December 30, 2009, he may still be considered a "lone wolf" for FISA warrants sought after the provision has expired. This grandfather clause is unaffected by the extension of the sunset date to December 31, 2009.

Roving Wiretaps

Section 206 of the USA PATRIOT ACT amended FISA to permit multipoint, or "roving," wiretaps by adding flexibility to the degree of specificity with which the location or facility subject to electronic surveillance under FISA must be identified.[29] It is often colloquially described as allowing FISA wiretaps to target persons rather than places.

Background

Prior to enactment of § 206, the scope of electronic surveillance authorized by a warrant was limited in two ways. First, the location or facility that was the subject of surveillance had to be identified.[30] Second, only identifiable third-parties could be directed to facilitate electronic surveillance by the government.[31] Conducting electronic surveillance frequently requires the assistance of telecommunications providers, landlords, or other third-parties. Furthermore, telecommunications providers are generally prohibited from assisting in electronic surveillance for foreign intelligence purposes, except as authorized by FISA.[32] Therefore, limiting the class of persons who could be directed to assist the government by a FISA warrant effectively limited the reach of FISA warrants to known and identifiable locations. If the location or facility was unknown, the identity of the person who would need to assist the government could not have been specified on the warrant.

Section 206 and "Other Persons"

Section 206 of the USA PATRIOT ACT amended § 105(c)(2)(B) of FISA to provide that "in circumstances where the Court finds, based on specific facts provided in the application, that the actions of the target of the application may have the effect of thwarting the identification of a

[26] P.L. 108-458, § 6001(b).

[27] P.L. 109-177, § 103.

[28] P.L. 108-458, § 6001(b) (referencing PATRIOT Act sunset provision in P.L. 107-56, § 224(b)).

[29] P.L. 107-56, § 206, *codified at* 50 U.S.C. § 1805(c)(2)(B) (2008).

[30] *See* 50 U.S.C. § 1805(c)(1)(B) (2001) (requiring FISA warrants to specify the "nature and location of each of the facilities or places at which electronic surveillance will be directed").

[31] *See* 50 U.S.C. § 1805(c)(2)(B) (2001).

[32] *See* 50 U.S.C. §§ 1809(a) and 1810 (2008).

specified person" a FISA warrant may direct "other persons" to assist with the electronic surveillance.[33] In a technical amendment later that year, the requirement that the warrant specify the location of the surveillance was also changed so that this requirement only applied if the facilities or places were known.[34] These modifications had the effect of permitting FISA warrants to direct *unspecified* individuals to assist the government in performing electronic surveillance, thus permitting warrants to authorize surveillance of places or locations that were unknown at the time the warrant was issued.

This section was further amended by the USA PATRIOT Improvement and Reauthorization Act of 2005 to require that the FISC be notified within 10 days after "surveillance begins to be directed at any new facility or place."[35] In addition, the FISC must be told the nature and location of each new facility or place, the facts and circumstances relied upon to justify the new surveillance, a statement of any proposed minimization procedures that differ from those contained in the original application or order, and the total number of facilities or places subject to surveillance under the authority of the present order.[36]

Particularity Requirement of the Fourth Amendment

The Fourth Amendment imposes specific requirements upon the issuance of warrants authorizing searches of "persons, houses, papers, and effects."[37] One of the requirements, referred to as the particularity requirement, states that warrants shall "particularly describ[e] the place to be searched."[38] Under FISA, roving wiretaps are not required to identify the location that may be subject to surveillance. Therefore, some may argue that roving wiretaps do not comport with the particularity requirement of the Fourth Amendment. Initially, it is not clear that the Fourth Amendment would require that searches for foreign intelligence information be supported by a warrant,[39] but prior legal challenges to similar provisions of Title III of the Omnibus Crime Control and Safe Streets Act (Title III) may be instructive in the event that challenges to § 206 are brought alleging violations of the particularity requirement of the Fourth Amendment.

Similar roving wiretaps have been permitted under Title III since 1986, in cases where the target of the surveillance takes actions to thwart such surveillance.[40] The procedures under Title III are similar to those currently used under FISA, but two significant differences exist. First, a roving wiretap under Title III must definitively identify the target of the surveillance.[41] Fixed wiretaps under Title III and all wiretaps under FISA need only identify the target if the target's identity is known. FISA permits roving wiretaps via warrants that only provide a specific description of the

[33] P.L. 107-56, § 206, *codified at* 50 U.S.C. § 1805(c)(2)(B) (2008).

[34] P.L. 107-108, § 314(a)(2)(A).

[35] P.L. 109-177, § 108(b)(4), *codified at* 50 U.S.C. § 1805(c)(3) (2008). This deadline for notification can be extended to up to 60 days by the FISC upon a showing of good cause.

[36] *Id.*

[37] U.S. CONST. amend. IV. The Supreme Court has held that electronic surveillance of private conversations qualifies as a search for purposes of the Fourth Amendment.

[38] *Id.*

[39] *See supra* footnote 5.

[40] Electronic Communications Privacy Act of 1986, P.L. 99-508, § 106(d)(3), *codified at* 18 U.S.C. § 2518(11) (2008).

[41] 18 U.S.C. § 2518(11)(b)(ii) (2008).

target.[42] Second, Title III requires that the surveilled individuals be notified of the surveillance, generally 90 days after surveillance terminates.[43] FISA contains no similar notification provision.

In *United States v. Petti*, the Ninth Circuit was presented with a challenge to a roving wiretap under Title III alleging that roving wiretaps do not satisfy the particularity requirement of the Fourth Amendment.[44] The Ninth Circuit initially noted that

> the test for determining the sufficiency of the warrant description is whether the place to be searched is described with sufficient particularity to enable the executing officer to locate and identify the premises with reasonable effort, and whether there is any reasonable probability that another premise might be mistakenly searched.[45]

Applying this test, the Ninth Circuit held that roving wiretaps under Title III satisfied the particularity clause of the Fourth Amendment.[46] The court in this case relied upon the fact that targets of roving wiretaps had to be identified and that they were only available where the target's actions indicated an intent to thwart electronic surveillance.[47]

Critics of roving wiretaps under FISA may argue that § 206 increases the likelihood that innocent conversations will be the subject of electronic surveillance. They may further argue that the threat of these accidental searches of innocent persons is precisely the type of injury sought to be prevented by the particularity clause of the Fourth Amendment. Such a threat may be particularly acute in this case given the fact that there is no requirement under FISA that the target of a roving wiretap be identified, although the target must be specifically described.[48]

Sunset

Section 206 of the USA PATRIOT ACT was initially set to sunset on December 31, 2005.[49] But, it was extended by the USA PATRIOT Improvement and Reauthorization Act of 2005 until December 31, 2009. After this date, § 105(c)(2) of FISA will read as it read on October 25, 2001,[50] eliminating the authority for FISA warrants to direct other unspecified persons to assist with electronic surveillance.[51]

---

[42] *See* 50 U.S.C. §§ 1804(a)(3), 1805(c)(1)(A) (2008).

[43] 18 U.S.C. § 2518(8)(d) (2008). This notification may be postponed upon an ex parte showing of good cause.

[44] *U.S. v. Petti*, 973 F.2d 1441, 1443-5 (9th Cir. 1992).

[45] *Id.* at 1444 (internal quotation marks omitted).

[46] *Id.* at 1445.

[47] *Id. See also*, *United States v. Bianco*, 998 F.2d 1112, 1124 (2nd Cir. 1993) (similarly holding that a similar provision authorizing roving bugs under Title III was constitutional).

[48] 50 U.S.C. §§ 1804(a)(3), 1805(c)(1)(B) (2008).

[49] P.L. 107-56, § 224(a).

[50] P.L. 109-177, § 102(b). The relevant section of FISA will then provide

> that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance. 50 U.S.C. § 1805(c)(2) (2001).

[51] The sunset will not repeal the provision of FISA that permits a FISA warrant to fail to identify facilities or places that (continued...)

The original sunset provision also provided a grandfather clause for investigations that began, or potential offenses that took place, before the date of the provision's expiration.[52] For example, if an individual is engaged in international terrorism on December 30, 2009, he may be the target of a roving wiretap under FISA even after authority for new roving wiretaps has expired. This grandfather clause is unaffected by the extension of the sunset date to December 31, 2009.

Access to Business Records Under FISA

Section 215 of the USA PATRIOT ACT enlarged the scope of documents that could be sought under FISA, as well as lowered the standard required before a court order could be issued compelling the production of documents.

Background

In 1976, the Supreme Court held that an individual's bank account records did not fall within the protection of the Fourth Amendment's prohibition on unreasonable searches and seizures.[53] Subsequently, Congress passed laws protecting various types of transactional information, but built in exceptions providing some access to statutorily protected records for counter intelligence purposes. [54] Similar statutory protections were also enacted for electronic communications records and credit bureau records.[55] As with financial records, these later statutes also included exceptions for access to records relevant to counter intelligence investigations. These exceptions comprise the authority for so-called national security letters (NSL), which can be used to compel the production of certain types of records.

In 1998, Congress amended FISA to provide access to certain records that were not available through NSL's.[56] Specifically, it created a mechanism for federal investigators to compel the production of records from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities.[57] Applications for orders under this section had to be made by FBI agents with a rank of Assistant Special Agent in Charge or higher and investigations could not be conducted solely on the basis of activities protected by the First Amendment.[58] Under these procedures the FISC would issue an order if, *inter alia*, the application contained "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[59] Recipients of an order under this section were required

(...continued)

will be subject to electronic surveillance. However, the authority for most new roving wiretaps may be effectively repealed because new orders may not direct unspecified persons to assist with surveillance.

[52] P.L. 107-56, § 224(b).

[53] *U.S. v. Miller*, 425 U.S. 435 (1976).

[54] *See* CRS Report RL33320, *National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments*, by Charles Doyle, at 3.

[55] *Id.* at 3-4.

[56] P.L. 105-272, tit. VI, § 602.

[57] 50 U.S.C. § 1862(a) (2001).

[58] 50 U.S.C. § 1862(a)(1) (2001).

[59] 50 U.S.C. § 1862(b)(2)(B) (2001).

to comply with it, and were also prohibited from disclosing to others that an order had been issued.[60]

Expansion of Scope of Documents Subject to FISA

In 2001, § 215 of the USA PATRIOT ACT made several changes to the procedures under FISA for obtaining business records.[61] Among these was an expansion of the scope of records that were subject to compulsory production. Whereas, prior to enactment of the USA PATRIOT ACT, only records from four explicit categories of businesses could be obtained, § 215 applied to "any tangible things."[62]

This expanded scope drew strong opposition from the library community, so much so that § 215 came to be known as the "library provision" despite the fact that the original text of the provision did not mention libraries.[63] Opposition from this group appears to have been primarily based upon the chilling effect such access could have on the exercise of First Amendment rights and purported intrusions into areas protected by the Fourth Amendment.[64] Opposition from library advocates may have also been a residual response to prior attempts by the FBI to gather foreign intelligence information from library staff and records during the Cold War.[65]

In response to these concerns, a library-specific amendment was made to the § 215 procedures by the USA PATRIOT Improvement and Reauthorization Act of 2005. Under this amendment, if the records sought were "library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person," the application has to be approved by one of three high-ranking FBI officers.[66]

Changes to the Standard of Review

Section 215 of the USA PATRIOT ACT also modified the standard that had to be met before an order compelling production of documents could issue from the FISC. Prior to enactment of § 215, an applicant had to have "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[67] In

[60] 50 U.S.C. § 1862(d)(1)-(2) (2001).

[61] P.L. 107-56, § 215 *codified at* 50 U.S.C. § 1862(a)-(b) (2008).

[62] 50 U.S.C. § 1861(a)(1) (2008).

[63] *E.g.* Richard B. Schmitt, *House Weakens Patriot Act's 'Library Provision'*, L.A. TIMES, June 16, 2005, at A-1.

[64] *See, e.g.*, AMERICAN LIBRARY ASSOCIATION, *Resolution on the USA Patriot Act and Related Measures That Infringe on the Rights of Library Users*, Jan. 29, 2003, available at http://www.ala.org; Judith King, Director ALA Office for Intellectual Freedom, Letter to the Editor, *FBI 'Fishing Expeditions' Librarians' Biggest Worry*, WALL ST. J., May 24, 2004, at A15; David Mehegan, *Reading Over Your Shoulder: The Push Is On To Shelve Part Of The Patriot Act*, BOSTON GLOBE, Mar. 9, 2004, at E5.

[65] *See* Ulrika Ekman Ault, *The FBI's Library Awareness Program: Is Big Brother Reading Over Your Shoulder?*, 65 N.Y.U. L. REV. 1532 (1990).

[66] Applications for these records could be made only by the Director of the Federal Bureau of Investigation, the Deputy Director of the Federal Bureau of Investigation, or the Executive Assistant Director for National Security. This authority cannot be further delegated. 50 U.S.C. § 1861(a)(3) (2008).

[67] 50 U.S.C. § 1862(b)(2)(B) (2001).

contrast, under § 215 as originally enacted, the applicant only needed to "specify that the records concerned [were] sought for a [foreign intelligence investigation.]"[68]

Subsequently, in 2005, Congress further amended FISA procedures for obtaining business records as part of the USA PATRIOT Improvement and Reauthorization Act of 2005. The applicable standard was again changed to require "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to a [foreign intelligence investigation.]"[69] Records are presumptively relevant if they pertain to

- a foreign power or an agent of a foreign power;
- the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or
- an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation;

Nondisclosure and Judicial Review

Orders issued under § 215 are accompanied by nondisclosure orders prohibiting the recipients from disclosing that the FBI has sought or obtained any tangible things pursuant to a FISA order. However, the recipient may discuss the order with other persons as necessary to comply with the order, with an attorney to obtain legal advice or assistance, or with other persons as permitted by the FBI. [70] The recipient must identify persons to whom disclosure has been made, or is intended to be made, if the FBI requests, except that attorneys with whom the recipient has consulted do not need to be identified.[71]

The USA PATRIOT Improvement and Reauthorization Act of 2005 also provided procedures for recipients of § 215 orders to challenge the judicial review of orders compelling the production of business records.[72] Once a petition for review is submitted by a recipient, a FISC judge must determine whether the petition is frivolous within 72 hours.[73] If the petition is frivolous, it must be denied and the order affirmed.[74] Otherwise the order may be modified or set aside if it does not meet the requirements of FISA or is otherwise unlawful.[75] Appeals by either party may be heard by the Foreign Intelligence Court of Review and the Supreme Court.[76]

Judicial review of nondisclosure orders operates under a similar procedure,[77] but such orders are not reviewable for one year after they are initially issued.[78] If the petition is not determined to be frivolous, a nondisclosure order may be set aside if there is

[68] P.L. 107-56, § 215.

[69] P.L. 109-177, § 106(b).

[70] 50 U.S.C. § 1861(d)(1) (2008).

[71] 50 U.S.C. § 1861(d)(2)(C) (2008).

[72] 50 U.S.C. § 1861(f)(2)(A)(i) (2008).

[73] 50 U.S.C. § 1861(f)(2)(A)(ii) (2008).

[74] *Id.*

[75] 50 U.S.C. § 1861(f)(2)(B) (2008).

[76] 50 U.S.C. § 1861(f)(3) (2008).

[77] Judicial review of nondisclosure orders was added by P.L. 109-178, § 3.

> no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.[79]

A petition to set aside a nondisclosure order may be defeated if the government certifies that disclosure would endanger the national security or interfere with diplomatic relations.[80] Absent any finding of bad faith, such a certification is to be treated as conclusive by the FISC. If a petition is denied, either due to a certification described above, frivolity, or otherwise, the petitioner may not challenge the nondisclosure order for another year.[81] Appeals by either party may be heard by the Foreign Intelligence Court of Review and the Supreme Court.[82]

DOJ OIG Report

The USA PATRIOT Improvement and Reauthorization Act of 2005 directed the Inspector General of the Department of Justice (OIG) to audit the FBI's use of § 215 authority and report its findings to Congress.[83] The OIG's most recent audit for calendar year 2006 was released in March of 2008.[84] According to that report, 21 applications for § 215 orders were made in 2006, of which six were withdrawn and 15 granted. The report also indicates that one of the six applications was withdrawn because the FISC indicated that it would not sign the order due to First Amendment concerns.[85]

Sunset

Section 215 of the USA PATRIOT ACT was initially set to sunset on December 31, 2005.[86] But, it was extended by the USA PATRIOT Improvement and Reauthorization Act of 2005 until December 31, 2009. After this date, § 501 and 502 of FISA will read as they read on October 25, 2001,[87] restricting the types of business records that are subject to FISA and reinstating the requirement for "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[88]

(...continued)

[78] 50 U.S.C. § 1861(f)(2)(A)(i) (2008).

[79] 50 U.S.C. § 1861(f)(2)(C)(i) (2008).

[80] Such certifications must be made by the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation. 50 U.S.C. § 1861(f)(2)(C)(ii) (2008).

[81] 50 U.S.C. § 1861(f)(2)(C)(iii) (2008).

[82] 50 U.S.C. § 1861(f)(3) (2008).

[83] P.L. 109-177, § 106A.

[84] OFFICE OF THE INSPECTOR GENERAL, DEP'T OF JUSTICE, *A Review of the FBI's Use of Section 215 Orders for Business Records in 2006*, Mar. 2008, available at http://www.usdoj.gov/oig/special/s0803a/final.pdf.

[85] *Id.* at 33. In indicating that it would deny the application, the FISC appears to have decided that "the facts were too 'thin' and that this request implicated the target's First Amendment rights." *Id.* at 68.

[86] P.L. 107-56, § 224(a).

[87] P.L. 109-177, § 102(b). Access will then be limited to records held by common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities. 50 U.S.C. § 1862(c)(2) (2001).

[88] 50 U.S.C. § 1862(b)(2)(B) (2001).

The original sunset provision also provided a grandfather clause for investigations that began, or potential offenses that took place, before the date of the provision's expiration.[89] For example, in the case of investigations that had already begun before December 30, 2009, a broader scope of records could be made accessible to the government under FISA even after the expiration date. This grandfather clause is unaffected by the extension of the sunset date to December 31, 2009.

Author Contact Information

Edward C. Liu
Legislative Attorney
eliu@crs.loc.gov, 7-9166

[89] P.L. 107-56, § 224(b).