

4 September 03

MEMORANDUM

From: Deputy Assistant Judge Advocate General (National Security Litigation and Intelligence Law)  
To: Judge Advocates

Subj: CODE 17 NEWS BULLETIN 03-03 - ANNOUNCEMENT OF NEW CODE 17 DIVISION DIRECTOR AND OVERVIEW OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) AND THE CHANGES IMPLEMENTED BY THE USA PATRIOT ACT

1. Purpose. This Bulletin announces the arrival of the new Code 17 Division Director and provides an introduction to FISA and an overview of the changes to FISA brought about by the USA Patriot Act.

2. Welcome Aboard. On 25 August 2003, CAPT James B. Norman, JAGC, USN, relieved CAPT DeLaney as Code 17 Division Director. CAPT Norman reports to Code 17 following his tour as Commanding Officer, NLSO North Central.

3. FISA Framework. The focus of this bulletin is on the portion of FISA that governs electronic surveillance of communications, although it should be noted that FISA governs several types of surveillance. Because most judge advocates are not familiar with the details of FISA, this bulletin provides a brief overview of the basic procedures before discussing changes to them.

a. FISA Purpose. FISA is the statute which authorizes federal agents to conduct electronic surveillance, as part of a foreign intelligence or counterintelligence investigation, without obtaining a traditional, probable-cause search warrant. The statute defines electronic surveillance as acquiring communications, by electronic or other means, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.<sup>1</sup> Although a traditional warrant is not required to conduct the surveillance, the statute establishes specific guidelines for when such surveillance is permissible, and vests the authority to approve the surveillance in an Article III judge.<sup>2</sup>

---

<sup>1</sup> 50 U.S.C. § 1801(f)

<sup>2</sup> 50 U.S.C. § 1803(a). FISA establishes the Foreign Intelligence Surveillance Court (FISC), made up of 11 district court judges, each eligible to hear and approve surveillance applications

b. FISA Standard. The standard for determining whether the surveillance will be authorized is probable cause to believe that the target is a foreign power or an agent of a foreign power.<sup>3</sup> This differs from the traditional standard (probable cause to believe evidence of a crime will be found) in recognition of the fact that intelligence investigations are not strictly concerned with investigating criminal activity, and often it may be difficult to identify a specific crime upon which to base a traditional warrant. In order to have a FISA surveillance application approved, the government also must certify that a "significant" purpose of the surveillance is to collect foreign intelligence information.<sup>4</sup> If the FISA court judge determines the government has met the standard, the judge will issue a FISA order authorizing the search.

c. FISA and the 4<sup>th</sup> Amendment. Of course, intelligence investigations often lead to criminal prosecutions of the targeted individuals based on evidence obtained during the surveillance. Thus, in order for the evidence to be admissible at trial, it is critical that the surveillance not violate the Fourth Amendment. Accordingly, the requirements of FISA are based on case law that dealt with foreign intelligence searches, and are designed to satisfy the Fourth Amendment. In an opinion that discusses the pre-FISA case law, the Second Circuit Court of Appeals stated that FISA strikes an appropriate balance between the individual's interest in privacy and the government's need to obtain foreign intelligence information. Although FISA surveillance authorizations are not based on the traditional standard of probable cause, FISA surveillances do not violate the Fourth Amendment.<sup>5</sup>

4. FISA Modifications. The USA Patriot Act, and subsequent related legislation, made several amendments to FISA. These include what is known as "roving authority;" extensions of several prescribed time periods; and a modification of the requirement that the surveillance be conducted for foreign intelligence purposes.

a. Roving Authority. FISA surveillance authorizations may now include "roving authority." Prior to the amendment, the law

---

<sup>3</sup> 50 U.S.C. § 1804(a)

<sup>4</sup> 50 U.S.C. §1804 (a)(7). The significant purpose standard is discussed further in paragraph 3c.

<sup>5</sup> *United States v. Duggan*, 743 F.2d 59, 74 (2d Cir. 1984). The court also noted that although the Supreme Court has not directly addressed this issue, in a pre-FISA case the Supreme Court stated that different standards may be compatible with the Fourth Amendment in light of the different purposes and practical considerations of domestic national security surveillances, *Id.*, at 72.

required the FISA court to specify the location of the surveillance and to name any third parties whose cooperation would be required, such as a telephone company or an internet service provider. If the target of the surveillance changed telephone companies, the government would have to return to the FISA court and request a supplemental order naming the new third party. With the change, the FISA court can now issue a generic order that can be served on any third party needed to assist with the surveillance.<sup>6</sup> This provides greater flexibility and reduces the chances of lost intelligence during the time required to obtain a supplemental order. In order to obtain this roving authority, the government must show that the target is likely to take steps to impede the advance identification of third parties. Also under the changes, third parties are explicitly immune from civil lawsuits arising from their compliance with a FISA court order.<sup>7</sup>

b. Extension of Time Periods. Prior to the amendments, the FISA court could approve an initial application for a period of 90 days, and in the case of a target that is a "foreign power,"<sup>8</sup> for a period of up to one year. Extensions could be authorized for the same 90-day or one-year time period as applicable. The amendments added a provision that allows an initial authorization period of 120 days in the case of targets that are "agents of foreign powers."<sup>9</sup> In those cases, after the initial 120-day period, extensions may be granted for up to one year. In addition, the time period for emergency authorizations was extended from 24 to 72 hours. If the attorney general determines an emergency situation exists, surveillance that would otherwise require court authorization may be conducted for up to 72 hours, during which time the government must either obtain court authorization or terminate the surveillance.<sup>10</sup>

c. Significant Purpose Test. The USA Patriot Act also modified the definition of the type of investigation in which a FISA order could be obtained. Previously, in order to obtain a FISA order, it was necessary that "the purpose" of the surveillance was to obtain intelligence information. With the change, the requirement now is that "a significant purpose" of the surveillance is to obtain intelligence information.<sup>11</sup> This is an important change because the original language had come to

---

<sup>6</sup> 50 U.S.C. § 1805(c)(2)

<sup>7</sup> 50 U.S.C. § 1805(i)

<sup>8</sup> "Foreign power" as defined in 50 U.S.C. § 1801(a).

<sup>9</sup> "Agent of a foreign power" as defined in 50 U.S.C. § 1801(b)

<sup>10</sup> 50 U.S.C. § 1805(f)

<sup>11</sup> 50 U.S.C. § 1804(a)(7)

be interpreted as "the primary purpose," and the government was required to show that gathering foreign intelligence, and not criminal prosecution, was the primary purpose of the surveillance. In order to meet this standard, the government endeavored to minimize any connection between the FISA surveillance request and a potential criminal prosecution. Over time, this led to the development of significant barriers and lack of communication between law enforcement and foreign intelligence.<sup>12</sup> With the change, it is now permissible for the primary purpose of the surveillance to be criminal prosecution, as long as gathering foreign intelligence remains a significant purpose. This is valuable because legitimate targets of foreign intelligence surveillance may also be involved in criminal activity, such as espionage or terrorism. These are both important objectives, and the government should not have to abandon one in order to pursue the other. The new language allows this by not requiring the government to declare which objective is primary.<sup>13</sup>

5. Security Announcement. Attention all NLSO and TSO Security Managers: Please provide your contact information to Mr. Jeremy Kulow, Code 17.11. As the security manager for Naval Legal Service Command, Mr. Kulow needs to maintain an updated list of the security managers for all subordinate commands. Mr. Kulow may be contacted at 202-685-5465; [KulowJS@jag.navy.mil](mailto:KulowJS@jag.navy.mil).

6. Points of Contact. CAPT James Norman, 202-685-5464, [NormanJB@jag.navy.mil](mailto:NormanJB@jag.navy.mil); LCDR John Bauer, at 202-685-5465, [BauerJD@jag.navy.mil](mailto:BauerJD@jag.navy.mil). The Code 17 office fax number is 202-685-5467 (DSN/325 for all telephone numbers).

J. B. NORMAN  
CAPT, JAGC, USN

---

<sup>12</sup> *In Re Sealed case No. 02-001*, 310 F.3d 717, 721 (U.S. Foreign Intelligence Court of Review, Nov 18, 2002).

<sup>13</sup> *Id.*, at 735. The court's opinion provides an in-depth discussion of the "significant purpose" test. The court concludes that the significant purpose test is valid and appropriate. The court went on to state that the "primary purpose" test was never required by the constitution or even the original FISA language.