"So Judge, How Do I Get That FISA Warrant?": The Policy and Procedure for Conducting Electronic Surveillance

Major Louis A Chiarella
Chief, Administrative Law
Office of the Staff Judge Advocate
Fort Carson, Colorado

Major Michael A. Newton
Professor, International and Operational Law Department
The Judge Advocate General's School, United States Army
Charlottesville, Virginia

Introduction

It's another slow Friday afternoon in the staff judge advocate's (SJA) office. Those individuals not out doing extended PT are enjoying another challenging game of solitaire. Things don't get much better for the new deputy SJA. Then the phone rings. The director of information management is talking in a muted voice. "Judge, I think I've got a problem with one of my system administrators. He has access to plenty of classified information on Army aircraft and ongoing operations. He hasn't been acting right since his car got repossessed last week. Plenty of hush-hush personal calls. And now I found out he's secretly copying files and taking documents home that are outside his area of responsibility. I know that he is very sympathetic to some of the foreign governments who are trying to upgrade their aviation assets. I think he may try to sell this information to a foreign power. Boy, that would cause some damage! During the SOLO course, I heard something about the requirements of FISA.[1] So Judge, how do I get that FISA warrant?"[2]

This hypothetical scenario is not all that unlikely. Army judge advocates confront intelligence law issues on a daily basis. The Army is a major collector, producer, and consumer of intelligence[3] and is one of thirteen agencies that comprise the Intelligence Community (IC).[4] The extensive statutory and regulatory framework governing intelligence activities demands constant and proactive legal involvement.

One of the most complex aspects of the framework is the Foreign Intelligence Surveillance Act (FISA). This article reviews the FISA and its implementing mechanism, which is contained in procedure 5 of *Department of Defense* (DOD) *Directive 5240.1-R*.[5] At the operational level, judge advocates need to have a clear understanding of when FISA authorization is necessary and what information is required by statute to obtain authorization. This article describes the step-by-step process for getting FISA authorization when required.

The Importance of Counterintelligence

No governmental interest is more fundamental than guaranteeing the security of the nation.[6] Only in a secure nation can the rights and liberties guaranteed by the Constitution be secure.[7] United States intelligence activities play a vital role in the protection of national security, and judges advocates must be familiar with the components of intelligence in order to understand the FISA.

One aspect of intelligence, foreign intelligence, focuses upon the collection and analysis of information about foreign

1. "FISA" is the common abbreviation for the Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511 (1978) (codified at 50 U.S.C. §§ 1801-1829 (1994)). The term SOLO refers to the Senior Officer Legal Orientation Course taught at the Judge Advocate General's School, U.S. Army, several times a year.

2. *See infra* notes 66-76 and accompanying text.

3. *See* Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *reprinted in* 50 U.S.C.A. § 401 (West 1996) [hereinafter EO 12,333]; *see also* U.S. CENTRAL INTELLIGENCE AGENCY, OPAI NO. 93-00092, A CONSUMER'S GUIDE TO INTELLIGENCE (1993) [hereinafter CONSUMER'S GUIDE] (copy on file with the authors).

4. CONSUMER'S GUIDE, *supra* note 3, at 28. Members of the United States Army routinely serve in four other IC agencies: the Defense Intelligence Agency, the National Security Agency, the National Reconnaissance Office, and the Central Imagery Office.

5. U.S. DEP'T OF DEFENSE, DIR. 5240.1-R, ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS (7 Dec. 1982) [hereinafter DOD DIR. 5240.1-R]. The Directive implements the requirements of *EO 12,333* within the DOD. Together, *EO 12,333* and *DOD Directive 5240.1-R* govern the collection of intelligence against United States persons, whether they are located within the United States or outside the United States. "[A]gencies are not authorized to use such techniques as electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency concerned and approved by the Attorney General." EO 12,333, *supra* note 3, para. 2.4. procedure 5 of *DOD Directive 5240.1-R* implements the requirements of the FISA.

6. *See* Haig v. Agee, 453 U.S. 280 (1981) (stating that it is "obvious and unarguable" that no governmental interest is more compelling than the security of the nation).

powers related to the conduct of United States governmental functions.[8] Foreign intelligence is offensive in nature, and primarily occurs outside the boundaries of the United States.

The defensive aspect of intelligence, known as counterintelligence, is of equal, if not greater, importance to national security than foreign intelligence is. The fundamental purpose of counterintelligence is protection against intelligence-gathering and covert activities directed against the United States by other countries.[9] Counterintelligence activities are designed to "discover, and where possible to counter, such clandestine activities of foreign intelligence services in order to protect United States military and diplomatic secrets as well as the integrity of United States governmental processes."[10] Counterintelligence can also have a very real impact upon United States citizens, as it frequently focuses on Americans who are suspected of collaborating with foreign agents.[11]

In an interesting statutory quirk, the FISA ignores conventional intelligence terminology and uses its own definitions. For example, the term "foreign intelligence information" in the FISA is a term of art which resembles the normal definition of counterintelligence.[12] Consequently, the first point of analysis for the judge advocate who seeks legal authority for electronic surveillance conducted for intelligence purposes is the determination of whether the information sought falls within the coverage of the FISA definition.[13]

---

7. Stephen A. Saltzburg, *National Security and the Fourth and Fifth Amendments, in* NATIONAL SECURITY LAW 1001 (John Norton Moore et al. eds., 1990) [hereinafter NATIONAL SECURITY LAW]; *see also* Stephen A. Saltzburg, *National Security and Privacy: Of Governments and Individuals Under the Constitution and the Foreign Intelligence Surveillance Act*, 28 VA. J. INT'L L. 129, 133 (1987) [hereinafter Saltzburg, *National Security and Privacy*] ("Personal liberty has prospered, both inside and outside U.S. courtrooms, because Americans have felt secure as a nation.").

8. Federal law defines foreign intelligence as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons." 50 U.S.C. § 401a(2) (1994). However, the provisions of procedure 5 of both *DOD Directive 5240.1-R* and *Army Regulation 381-10* apply to intelligence collection by DOD personnel, regardless of the target or location.

9. Counterintelligence collection is defined as: "The systematic acquisition of information on espionage, sabotage, terrorism, and related hostile intelligence activities conducted for, or on behalf of, foreign powers, organizations, or persons, that are directed against or threaten DOD interests." U.S. DEP'T OF DEFENSE, INSTR. 5240.10, DOD COUNTERINTELLIGENCE SUPPORT TO UNIFIED AND SPECIFIED COMMANDS, para. C1 (18 May 1990) [hereinafter DOD INSTR. 5240.10]. Despite the end of the Cold War, many countries still maintain massive organizations directed at the collection of intelligence and the conduct of covert actions of which the United States is a major target. *See generally* REPORT OF THE COMMISSION ON THE ROLES AND CAPABILITIES OF THE UNITED STATES INTELLIGENCE COMMUNITY, PREPARING FOR THE 21ST CENTURY: AN APPRAISAL OF U.S. INTELLIGENCE (MAR. 1, 1996) [hereinafter APPRAISAL]; *Current and Projected National Security Threats to the United States and its Interests Abroad: Hearings Before the Senate Select Comm. on Intelligence*, 104th Cong., 2d Sess. (1996).

10. Daniel B. Silver, *Intelligence and Counterintelligence, in* NATIONAL SECURITY LAW, *supra* note 7, at 913, 916. *See also* 50 U.S.C. § 401a(3) (The objective of counterintelligence is the gathering of information to protect against "espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorist activities.").

11. Reflecting the impact of counterintelligence, Americans have frequently challenged the intrusiveness of various forms of counter-intelligence surveillance as violating basic Constitutional rights. *See* Americo Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 817 n.126 (1989); *see also* U.S. v. Nicholson, 955 F. Supp. 588 (E.D. Va. 1997); Saltzburg, *National Security and Privacy*, *supra* note 7, at 130; Note, *The Foreign Intelligence Surveillance Act of 1978*, 13 VAND. J. TRANSNAT'L L. 719, 747-59 (1980). As of this writing, no federal or state court has found the requirements of the FISA to be in conflict with either statutory or constitutional rights of citizens. For some background to the privacy issues protected by the FISA, see *Final Report of the Senate Select Comm. To Study Governmental Operations With Respect to Intelligence Activities and the Rights of Americans, Book II*, S. REP. NO. 94-755, at 325 (1976) [hereinafter CHURCH COMM. REPORT].

In recognition of the constitutional rights of United States citizens, the FISA includes a requirement that the surveillance follow minimization procedures which are specified in the statute. 50 U.S.C.A. § 1801(h) (West 1997). The FISA also provides that no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the First Amendment to the Constitution. *Id*. § 1805 (a)(3)(A). In addition, the Attorney General must include a statement of the proposed minimization procedures when seeking a warrant from the Foreign Intelligence Surveillance Court (FISC). *Id*. § 1804(a)(5).

12. The FISA does not regulate the collection of foreign intelligence by United States agencies outside the United States. Within the United States, the term "foreign intelligence information" is specifically defined by statute. *See* 50 U.S.C.A. § 1801(e).

13. The FISA authorizes electronic surveillance or physical searches only when the certifying official is seeking "foreign intelligence information," as defined in the statute. *See id.* § 1802.

> "Foreign intelligence information" 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.

Id. § 1801(e).

Counterintelligence Versus Law Enforcement

As a practical matter, judge advocates must always remember that counterintelligence within the United States is distinct from domestic law enforcement. Counterintelligence and law enforcement are both necessary to protect society and to preserve democracy, but the similarity between the two ends there. Counterintelligence and law enforcement have different goals: providing for national security versus deterring and punishing criminal activity. As a result of the contrasting goals, counterintelligence and law enforcement employ different methods.[14] They also differ in the manner of disclosure to the subject of the surveillance. The subject of a law enforcement investigation eventually learns of or knows about any searches and surveillance, even if the collection of the evidence does not result in prosecution.[15] The "subject" of counterintelligence collection techniques will not learn of searches and surveillance conducted, except in those exceptional instances where the Attorney General later approves the use of the collected information as criminal evidence.[16]

The most important distinction between counterintelligence and law enforcement is that they differ in the uses of the information collected. The primary use of law enforcement information is the conduct of criminal prosecutions. The hallmarks of a law enforcement investigation are repeated conferences with the appropriate criminal prosecutor, concerted efforts to acquire specific information needed to prove each element of every charged offense at trial, and the deliberate collection of the evidence required to sustain the prosecutorial theory of the case. In contrast, the primary use of counterintelligence information is the conduct of United States foreign and national defense policies.[17] Guidance from the DOD specifically states that the purpose of counterintelligence collection is to detect espionage, sabotage, terrorism, and related hostile intelligence activities to "deter, [to] neutralize, or [to] exploit them."[18]

The purpose for collecting the information has great significance beyond merely distinguishing between counterintelligence and law enforcement. The primary purpose of the investigation determines the lawful procedures for collecting evidence. Counterintelligence collection may produce evidence which is ultimately used at trial and which will often provide reasonable belief that the targets have committed crimes. However, the primary purpose of any information collection effort is critical for ascertaining its legality at the time of initiation, as well as dictating the subsequent standard of legal review. Crossing the "primary purpose" line for information collection—from the pursuit of counterintelligence to law enforcement—subjects the investigation and evidence to extensive legal scrutiny and policy concerns.[19]

Within the United States, the Federal Bureau of Investigation (FBI) is the lead agency for conducting counterintelligence and coordinating the counterintelligence efforts of other agencies within the IC.[20] The FBI is also the lead agency for developing the evidence necessary for the Department of Justice

---

14. *See, e.g.*, U.S. DEP'T OF DEFENSE, DIR. 5505.09, INTERCEPTION OF WIRE, ELECTRONIC, AND ORAL COMMUNICATIONS FOR LAW ENFORCEMENT (20 April 1995). This DOD Directive specifically does not apply to "the interception of wire, electronic, and oral communications for counterintelligence or foreign intelligence, including information on the foreign aspects of narcotics production and trafficking." *Id*.

15. For criminal investigations, Federal Rule of Criminal procedure 41 requires that the target receive a copy of the warrant and an inventory of seized property. Normal wiretaps and search warrants are ultimately made public, even if criminal charges do not result. JIM MCGEE & BRIAN DUFFY, MAIN JUSTICE: THE MEN AND WOMEN WHO ENFORCE THE NATION'S CRIMINAL LAWS AND GUARD ITS LIBERTIES 325 (1996); Daniel J. Gallington, Deputy Counsel for Intelligence Policy, Office of Intelligence Policy and Review, U.S. Department of Justice, Address in Washington, D.C. (Dec. 1, 1994) [hereinafter Gallington] (notes from this speech are on file with the authors).

16. The fruits of counterintelligence investigations can become part of criminal prosecutions, but most counterintelligence investigations do not result in criminal prosecutions and receive little or no public disclosure. MCGEE & DUFFY, *supra* note 15, at 303. The decision to pursue a criminal case following the termination of the counterintelligence investigation involves a delicate balancing test. The Attorney General must determine when the benefit of criminal prosecution outweighs the impact of revealing the existence and effectiveness of American electronic surveillance efforts. Gallington, *supra* note 15. In the context of electronic surveillance, the statute requires the federal district court judge, upon a motion by the accused to suppress evidence obtained under the FISA, to:

> 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.

50 U.S.C.A. § 1806(f).

In the context of courts-martial, this statutory requirement means that the trial judge will have to delay the military proceedings pending a determination of the legality of the FISA warrant and its subsequent evidence. *See, e.g.*, U.S. v. Ott, 637 F. Supp. 62 (E.D. Cal. 1986). Airman Ott was convicted at a general court martial and sentenced to a dishonorable discharge, total forfeitures, reduction to airman basic, and 25 years confinement. U.S. v. Ott, 26 M.J. 542 (A.F.C.M.R. 1988). *See also* U.S. v. Horton, 17 M.J. 1131 (N.M.C.M.R. 1984).

17. "In law enforcement, the purpose of surveillance is to prosecute the guilty. In intelligence, the purpose of surveillance is to gather information which should not be used for or against any individual, but to safeguard the country from foreign enemies." S. REP. NO. 97-691, at 9-10 (1982).

18. DOD INSTR. 5240.10, *supra* note 9, para. C1.

(DOJ) to prosecute espionage cases.[21] To maintain the proper "primary purpose" during counterintelligence investigations, the Attorney General's guidelines require the Office of Intelligence Policy and Review to approve all contacts between the FBI and the DOJ Criminal Division attorneys.[22]

The distinction between intelligence collection and law enforcement is fundamental. For judge advocates, the primary purpose line determines whether *DOD Directive 5240.1-R* (and its implementation in *Army Regulation 381-10*) even applies. Components of the DOD cannot use the procedures for collecting intelligence information as a subterfuge for collecting evidence for a prosecutorial purpose.[23]

Counterintelligence Versus Domestic Security

Counterintelligence within the United States is also distinct from domestic security. Domestic security involves protecting the state from internal threats that do not have connections with oreign powers or international organizations.[24] As a result, domestic security functions lie in the middle ground between counterintelligence and the normal preparation of criminal cases. Threats posed by domestic organizations which seek to attack and to subvert the existing structure of government can be as grave as those involving foreign powers.[25] The absence of a foreign power linkage, however, prevents the use of the FISA mechanism to collect counterintelligence information.

The critical distinction for judge advocates is whether the information collection requires a warrant under normal criminal procedures.[26] The United States Constitution requires the issuance of a warrant to conduct all electronic surveillance for domestic security criminal investigations. However, courts reviewing the methods employed to secure the nation have balanced the "[g]overnment's right to protect itself from unlawful subversion and attack" against "the citizen's right to be secure in his privacy against unreasonable government intrusion."[27]

In *United States v. United States District Court* (generally referred to as the *Keith* case), the United States Supreme Court determined that no safeguards other than appropriate prior warrant procedures satisfy the Fourth Amendment for domestic security matters.[28] The underlying rationale for this holding is

---

19. McGee & Duffy, *supra* note 15, at 321-43. *See* U.S. v. Pelton, 835 F.2d 1067 (4th Cir. 1987), *cert. denied*, 486 U.S. 1010 (1986); U.S. v. Butenko, 494 F.2d 593, 605 (3d. Cir. 1974), *cert. denied*, 491 U.S. 881 (1974) (Even though the warrantless surveillance collected the conversations of American citizens, it was deemed lawful because: (1) the "primary purpose" of the surveillance was to obtain foreign intelligence information and (2) the efficiency of the nation's intelligence process would be lost if courts required intelligence operatives to interrupt collection and "rush to the nearest available magistrate.").

The FBI is keenly aware of the distinction between law enforcement (and its corollary of preparing criminal cases) and the collection of intelligence information. The distinction touches every facet of a criminal case and affects such issues as what information must be turned over pursuant to the Jencks Act, which attorneys within the Department of Justice make those decisions, which attorneys in which offices review applications under the FISA, and which policymakers decide on the disposition of criminal cases which touch on national security matters. The United States Court of Appeals for the Fourth Circuit originally articulated the test for reviewing the use of information gathered using electronic surveillance in subsequent criminal prosecutions. United States v. Truong Dinh Hung, 629 F.2d 908, 915-16 (4th Cir. 1980), *cert. denied*, 454 U.S. 1144 (1982) (based on facts which predated the FISA). In upholding the primary purpose propounded by the government, the court rejected the appellant's claim that an electronic surveillance would be lawful in the absence of a warrant only where the purpose was "'solely' for foreign policy reasons." *Id*.

20. EO 12,333, *supra* note 3, pt. 1.14.

21. The Central Intelligence Agency (CIA) is precluded from conducting electronic surveillance within the United States except for the purposes of training, testing, or conducting countermeasures to counter hostile electronic surveillance. *Id*. pt. 2.4(a). The National Security Act specifies that the CIA "shall have no police, subpoena, or law enforcement powers or internal security functions." 50 U.S.C.A. § 403-3(d)(1) (West 1997).

22. McGee & Duffy, *supra* note 15, at 336. On 19 July 1995, Attorney General Reno issued a confidential four-page memorandum which established new rules of conduct for FBI agents and Criminal Division lawyers working on counterintelligence investigations and employing electronic surveillance under the FISA. *Id*. at 341. Under the new rules, the FBI and the Criminal Division are forbidden from contacting each other independently, and the FBI is further prohibited from contacting a U.S. Attorney's office without prior permission from both the Office of Intelligence Policy and Review and the Criminal Division of the DOJ. *Id*. Agents of the FBI who are working on counterintelligence investigations are also required to "maintain a log of all contact with the Criminal Division, noting the time and participants involved." *Id*. "The Criminal Division shall not . . . instruct the FBI on the operation, continuation, or expansion of FISA electronic surveillance or physical searches." *Id*.

23. DOD Dir. 5240.1-R, *supra* note 5, procedure 1, A, 3.

24. The Oklahoma City bombing, which involved no known connection to a foreign power or international organization, is an example of domestic security. *See* Commander Jim Winthrop, *The Oklahoma City Bombing: Immediate Response Authority and Other Military Assistance to Civil Authority (MACA)*, Army Law., July 1997, at 3. One characteristic which distinguishes national security from domestic security is the entity at which action is directed. National security involves government action directed at other nations (or foreign forces) and their agents, while domestic security involves government action directed at individuals. Saltzburg, *National Security and Privacy*, *supra* note 7, at 131.

25. For example, in *United States v. United States District Court*, 407 U.S. 297, 299 (1972), the United States charged three defendants with conspiracy to destroy Government property in violation of 18 U.S.C. § 371 and also charged one defendant with the dynamite bombing of the CIA office in Ann Arbor, Michigan. (This case is generally referred to as the *Keith* case.).

26. *See generally* 18 U.S.C. §§ 2510-20 (1994).

that warrantless electronic surveillance does not pass the reasonableness test of the Fourth Amendment with regard to internal security.[29] The Supreme Court, however, expressly declined to address whether the domestic security warrant requirements also applied to the surveillance of foreign governments or their agents.[30] Without waiting for Supreme Court clarification regarding the proper line between national security concerns and personal privacy when foreign governments or their agents are involved, Congress passed the FISA as a legal mechanism to serve both purposes.

What is the FISA?

On 25 October 1978, President Carter signed the FISA into law. The explicit purpose of the FISA was to balance the protection of individual privacy with the needs of national security through the development of a regulatory framework for certain counterintelligence activities of the executive branch of the federal government.[31] Many factors necessitated this express balancing act. First, the Supreme Court's decision in *Keith* did not address the extent of the executive's constitutional powers in the area of counterintelligence.[32] Writing for the majority, Justice Powell explicitly stated that the opinion made no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers or their agents.[33] Second, congressional hearings revealed that both the FBI and the Central Intelligence Agency (CIA) had operated outside the law, in the name of intelligence collection.[34] The Church Committee[35] realized that counterintelligence was essential to the preservation of American civil liberties, and it recognized the need to collect intelligence and to establish appropriate limits on intrusive investigative techniques.[36] Through the efforts of key officials from the DOJ and the Church Committee,[37] the FISA became "the gold standard of legality in the world of counterintelligence."[38]

---

27. *Keith*, 407 U.S. 297. *See also* Halperin v. Kissinger, 807 F.2d 180 (D.C. Cir. 1986) (holding that a purportedly political motive for a warrantless wiretap of a national security staffer was irrelevant if an objectively reasonable national security rationale was also present); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974) ("the President's . . . inherent power to protect national security in the conduct of foreign affairs" authorized "warrantless wiretaps for the purpose of gathering foreign intelligence").

28. *Keith*, 407 U.S. at 309. The Supreme Court in *Keith* also determined that the President's constitutional powers to protect the government against those who would subvert or overthrow it by unlawful means did not include warrantless searches in connection with domestic security matters. *Id.*

29. *Id*. at 315. The Supreme Court recognized that domestic security, with its ongoing intelligence gathering activities, was different from "ordinary crime." *Id.* at 322. Accordingly, domestic security is not subject to the requirements of Title III of the Omnibus Crime Control and Safe Streets Act, Pub. L. No. 90-351, 82 Stat. 212 (1968) (codified as amended at 18 U.S.C. §§ 2510-20 (1994)), which regulates electronic surveillance for ordinary federal crimes. The Supreme Court's recognition that a less precise standard was acceptable even for domestic security investigations gave impetus to subsequent legislation and judicial determinations that warrantless surveillance was permissible for national security investigations involving foreign powers and their agents. Cinquegrana, *supra* note 11, at 805.

30. *Keith*, 407 U.S. at 321-22, n. 20.

31. The FISA does not extend to all types of intelligence gathering. As originally enacted, the FISA did not apply to physical searches of real and personal property. *See In re* Application of the United States for an Order Authorizing the Physical Search of Nonresidential Premises and Personal Property, slip op. (U.S. For. Intell. Surveillance Ct., June 11, 1981). In the wake of the Aldrich Ames case, Congress amended the FISA to include physical searches conducted "to obtain foreign intelligence information." 50 U.S.C.A. § 1823(a)(7) (West 1997). *See* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807 (codified at 50 U.S.C. §§ 1821-29). The FISA covers neither the electronic surveillance of United States persons who are abroad nor "watch listing" that targets the international communications of foreign nationals who are in the United States. *See* 50 U.S.C.A. § 1801(f)(1). The lack of regulation under the FISA does not mean that some intelligence collection techniques are unregulated. The approval of the Attorney General is required for any technique used for intelligence purposes which would require a warrant if it were undertaken for a law enforcement purpose. EO 12,333, *supra* note 3. Additionally, the DOD regulates all DOD electronic surveillance for intelligence purposes, regardless of location, technique, or target. DOD. DIR. 5240.1-R, *supra* note 5, procedure 5.

32. The FISA, an authorization of Congress, increased the President's power in this area:

> When the President acts pursuant to an expressed or implied authorization of Congress, his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate . . . . A seizure executed by the President pursuant to an act of Congress would be supported by the strongest of presumptions and the widest latitude of judicial interpretation, and the burden of persuasion would rest heavily upon any who might attack it.

Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635-37 (1952) (Jackson, J., concurring).

33. *Keith*, 407 U.S. at 322.

34. CHURCH COMM. REPORT, *supra* note 11.

35. *See* APPRAISAL, *supra* note 9, app. A (providing an overview of the role of the Church Committee in the evolution of the United States intelligence community).

36. MCGEE & DUFFY, *supra* note 15, at 310. The Church Committee also recognized the need for a "wall" between federal law enforcement and the nation's intelligence community. *Id.*

37. *Id.* at 310-13.

The FISA is a complex statute, with an elaborate structure and flexible procedures.[39] It is not, however, a comprehensive statute for all intelligence activities. The FISA regulates counterintelligence investigations;[40] it does not extend to domestic security investigations. The FISA also regulates specific counterintelligence collection techniques—primarily "electronic surveillance,"[41] but physical searches as well. Other intelligence collection techniques have separate statutory and regulatory provisions.[42] Additionally, the FISA has no extraterritorial applicability;[43] therefore, it does not regulate the use of electronic surveillance outside of the United States. Because of the limited application under the FISA, there are other statutory and regulatory sources which control other counterintelligence activities.

All electronic surveillance for counterintelligence purposes within the United States is subject to the requirements of the FISA. This does not mean, however, that prior judicial authorization is always required. The Attorney General may acquire foreign intelligence information for periods up to a year without a judicial order if the Attorney General certifies in writing under oath that:

> (A) the electronic surveillance is solely directed at . . . communications used exclusively between or among foreign powers[44]. . . [or] technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power . . .;
> (B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and (C) the proposed minimization procedures[45] . . . meet [the statutory definition] of minimization procedures . . . .[46]

The FISA establishes a much more stringent standard in circumstances involving the electronic surveillance of "United States persons."[47] In such circumstances, the Executive may conduct electronic surveillance only pursuant to the FISA's procedures for judicial review and approval.[48] Each application for a surveillance order must include, inter alia:

> 1) the identity of the federal officer making the application;
> 2) the authority conferred on the Attorney General by the President of the United States and the approval of the Attorney General to make the application;
> 3) the identity, if known, or a description of the target of the electronic surveillance;
> 4) a statement of the facts and circumstances relied upon by the applicant to justify his belief that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power . . . [and] each of the facilities

38. *Id.* at 315.

39. "The elaborate structure of [the FISA] demonstrates that the political branches need great flexibility to reach the compromises and [to] formulate the standards which will govern foreign intelligence surveillance." United States v. Truong Dinh Hung, 629 F.2d 908, 914 n.4 (4th Cir. 1980).

40. The statute actually uses the term "foreign intelligence information," but it still refers to information necessary to protect the United States from the acts of foreign powers and their agents. 50 U.S.C.A. § 1801(e) (West 1997).

41. There are four categories of "electronic surveillance"—watch listing, wiretaps, radio intercepts, and monitoring devices. *Id.* § 1801(f). The statutory definition encompasses communications within the United States "under circumstances where the person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." *Id.* Although the FISA governs intelligence collection of the contents of communications, federal law stretches the FISA to cover other electronic surveillance such as pen registers, trap, and trace devices. 18 U.S.C.A. § 3121 (West 1996).

42. EO 12,333, *supra* note 3; U.S. DEP'T OF ARMY, REG. 381-10, U.S. ARMY INTELLIGENCE ACTIVITIES (1 July 1984) [hereinafter AR 381-10].

43. A general presumption against the extraterritorial application of statutes exists in American jurisprudence. Equal Employment Opportunity Comm'n v. Arabian Am. Oil Co., 499 U.S. 244 (1991). The primary purpose of this presumption against extraterritoriality is "to protect against the unintended clashes between our laws and those of other nations which could result in international discord." *Id*. at 248.

44. *See* 50 U.S.C.A. § 1801(a) (defining "foreign power").

45. Minimization procedures are measures adopted by the Attorney General that are reasonably designed to minimize the acquisition and retention, and to prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons. *Id.* § 1801(h). Detailed minimization procedures adopted by the Attorney General are classified. Telephone Interview with John Petrow, Office of Intelligence Policy and Review, U.S. Dep't of Justice (Dec. 11, 1996) [hereinafter Petrow Interview] (notes on file with authors).

46. 50 U.S.C.A. § 1802(a)(1) (citations omitted). It is the policy, however, of the present Attorney General to seek judicial approval for the use of electronic surveillance within the United States involving non-U.S. persons. Petrow Interview, *supra* note 45.

47. 50 U.S.C.A. § 1801(i). The more stringent procedures of the FISA apply in all instances which do not involve an acknowledged foreign power or its agents. *Id.* § 1802(b).

48. *Id.* The Attorney General may, however, authorize immediate surveillance in times of emergency. The Attorney General must "as soon as practicable, but not more than twenty-four hours" later, seek judicial review of the emergency application. *Id.* § 1805(e).

> or places [to be subjected to the surveillance] . . . is being used, or is about to be used, by a foreign power or an agent of a foreign power;
> 5) a statement of the proposed minimization procedures;[49]
> 6) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance; [and]
> 7) a certification [from an appropriate executive branch official] . . . that the certifying official deems the information sought to be foreign intelligence information . . . that the purpose of the surveillance is to obtain foreign intelligence information . . . that such information cannot reasonably be obtained by normal investigative techniques . . . .[50]

The application must also contain statements regarding all previous applications involving the target, the means by which the surveillance will be implemented (including whether physical entry[51] is required to effect the surveillance), and the anticipated duration.[52]

Each application approved by the Attorney General for the electronic surveillance of United States persons within the United States must have judicial approval. The Chief Justice of the United States Supreme Court has designated seven federal district court judges to be the Foreign Intelligence Surveillance Court (FISC) and to review the electronic surveillance search applications.[53] A FISC judge will approve the electronic surveillance application and issue an ex parte order[54] upon a finding that: (1) "the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;"[55] (2) an authorized federal official made the application and the application was "approved by the Attorney General;"[56] (3) there is probable cause to believe that the target is "a foreign power or an agent of a foreign power" and that each place subjected to surveillance "is being used, or is about to be used, by a foreign power or an agent of a foreign power;"[57] (4) "the proposed minimization procedures meet the [statutory] definition of minimization procedures . . . ;"[58] and (5) all required statements are contained in the application and, "if the target is a United States person, the [statutory] certification or certifications are not clearly erroneous . . . ."[59]

Despite almost twenty years of implementation and thousands of applications, the FISC has not denied a single government request for electronic surveillance.[60] Opponents of the

---

49. A copy of the minimization procedures adopted by the Attorney General remain on file with the Foreign Intelligence Surveillance Court. Petrow Interview, *supra* note 45. The FISA application may include additional minimization procedures to protect the privacy of persons who are not the target of the requested electronic surveillance. *Id.*

50. 50 U.S.C.A. § 1804(a)(1)-(7). The executive branch official must include a statement of facts to support his certifications. *Id.* § 1804(a)(7)(E). The purpose of this certification is to ensure that a national security wiretap is being sought for "intelligence purposes" and not to obtain evidence for a criminal case through the backdoor of a counterintelligence inquiry. McGee & Duffy, *supra* note 15, at 318. *See* Exec. Order No. 12,139, 44 Fed. Reg. 30,311 (1979), *reprinted in* 50 U.S.C.A. § 1803 note (setting forth the executive branch officials who are designated to make the certifications required by 50 U.S.C.A. § 1804(a)(7) in support of electronic surveillance applications). The officials designated by executive order include the Secretary and Deputy Secretary of Defense, the Director and Deputy Director of the Central Intelligence Agency, and the Director of the Federal Bureau of Investigation. Within the Department of Defense, certification authority has been delegated to the Secretary and Under Secretary of each military department and to the Director of the National Security Agency. DOD Dir. 5240.1-R, *supra* note 5, procedure 5, pt.1(B)(2).

51. The FISA has been amended to include physical searches of real and personal property. *See supra* note 31; McGee & Duffy, *supra* note 15, at 321, 342. *See also* U.S. v. Nicholson, 955 F. Supp. 588 (E.D. Va. 1997) (upholding the physical search provisions of the FISA against a Fourth Amendment challenge).

52. 50 U.S.C.A. § 1804(a)(8)-(10).

53. *Id.* §§ 1803-04.

54. The FISC order often includes secondary orders to phone companies, directing these entities to provide facilities and information to the intelligence agency identified in the primary order. Petrow Interview, *supra* note 45.

55. 50 U.S.C.A. § 1805(a)(1).

56. *Id.* § 1805(a)(2).

57. *Id.* § 1805(a)(3).

58. *Id.* § 1805(a)(4) (citation omitted).

59. *Id.* § 1805(a)(5) (citation omitted).

60. McGee & Duffy, *supra* note 15, at 318; Gallington, *supra* note 15. Through the end of 1995, there were 8,812 orders issued under the FISA (one case, however, can generate multiple orders). Electronic Privacy Information Center, *Foreign Intelligence Surveillance Act Orders 1979-1995* (visited Apr. 28, 1997) <http://www.epic.org/privacy/wiretap/fisa_stats.html>. Through the first half of 1996, the DOJ was on a pace to process more than 800 requests for FISA orders. Jim McGee and Brian Duffy, *Someone to Watch Over Us*, Wash. Post Magazine, June 23, 1996, at 9, 11.

FISC question its impartiality[61] and the underlying reasoning by which courts have accepted the statute's constitutionality.[62] Every United States federal district and circuit court that has conducted independent reviews of FISC authorizations has held that they are both lawful and constitutional.[63]

Despite the utility of the FISA as an investigative tool, trial counsel should remember that electronic surveillance is only one component of the wider investigative arsenal. The intelligence investigation as a whole develops in accordance with established execution channels within the military intelligence community. The FISA approval channels are distinct and will often involve governmental agencies other than those that are part of the overall mechanism for conducting the intelligence investigation.

So Who is the Approval Authority?

The FISA is not an all encompassing source of approval for all intelligence-gathering situations. As noted earlier, the FISA only regulates the collection of information about activities involving a foreign power or an agent of a foreign power. Additionally, the FISA does not regulate all of the collection techniques employed for counterintelligence investigations. The use of concealed monitoring, searches and examinations of mail, physical surveillance, and undisclosed participation in organizations all have separate approval schemes. Even for some cases of electronic surveillance and physical searches employed for counterintelligence purposes, other provisions of procedure 5 may substitute for the FISA as a source of approval for the military practitioner.

So who approves electronic surveillance? The approval authority for the use of electronic surveillance fluctuates with the type of person, the location, and the type of situation involved. The approval level for the use of electronic surveillance and counterintelligence physical searches ranges from the unit commander to prior judicial review and endorsement. While the importance and intrusiveness of electronic surveillance remains constant, different expectations of privacy cause the approval level to change. In ascending order, the levels of approval authority are:

Table of Electronic Surveillance Approval Authority

Outside of the United States:

Type of Entity	Approval Authority	Source(s) of Authority
Non-U.S. person	Commanding General, Intelligence & Security Command and Designated Commanders[64]	AR 381-10, proc. 5, pt. 2: F
Emergency,[65] U.S. person	Secretary & Deputy Secretary of Defense; Secretary and Under Secretary of the Army; Director & Deputy Director, National Security Agency; and General Officers[66]	DOD Dir. 5240.1-R, proc. 5, pt. 2: D, E
U.S. person	Attorney General[67]	Exec. Order 12,333, para. 2.5, DOD Dir. 5240.1-R, proc. 5, pt. 2: C

Inside the United States:[68]

61. *See, e.g., Foreign Intelligence Surveillance Act: Oversight: Hearings Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the House Comm. on the Judiciary*, 98th Cong. 27 (1983) [hereinafter *Hearings*] (testimony of Mark Lynch, Attorney, ACLU) (the FISC was viewed as a captive of the national security establishment).

62. *See* Gregory E. Birkenstock, *The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis*, 80 GEO. L.J. 843, 849-50 (1992) (examining the FISA probable cause standard in terms of an administrative search instead of as an exception to the warrant clause).

63. *Hearings*, *supra* note 61, at 6-7 (testimony of Mary C. Lawton, Office of Intelligence Policy and Review, DOJ).

64. The Assistant Chief of Staff for Intelligence, Headquarters, Department of the Army; the Commander in Chief, U.S. Army, Europe and Seventh Army; the Commanding General, Eighth United States Army; and the Commanding General, Intelligence and Security Command, may approve electronic surveillance by Army intelligence components. All four officials may delegate authority to their deputies, chiefs of staff, or ranking intelligence staff officers; they, in turn, may delegate their authority to the responsible military intelligence group commanders. AR 381-10, *supra* note 42, procedure 5, pt. 2(F).

65. Emergency surveillance cannot last longer than the time required to obtain Attorney General approval of the collection, and in no event may it last longer than 72 hours without Attorney General approval. DOD DIR. 5240.1-R, *supra* note 5, procedure 5, pt. 2(D)(4). For the purposes of electronic surveillance, "emergency" means a situation where securing prior approval of the Attorney General is not practical because the time delay would cause substantial harm to national security, a person's life is reasonably believed to be in immediate danger, or the physical security of a defense installation or government property is reasonably believed to be in immediate danger. *Id*. Except for cases involving immediate danger to a person's life or physical safety, the certifying official must find probable cause to link the surveillance to collection against a foreign power using one of the five specific categories of activity. *Id.* pt. 2(C)(2)(a).

66. Authorization for emergency electronic surveillance may be granted by "[a]ny general or flag officer at the overseas location in question, having responsibility for either the subject of the surveillance, or responsibility for the protection of the persons, installations, or property that is endangered," or by the Deputy Director for Operations of the National Security Agency. *Id.* pt. 2(E)(2).

67. The Attorney General applies the same standards for approval of electronic surveillance involving U.S. persons abroad that the FISC applies to U.S. persons within the United States. The Attorney General executes a memorandum as the method for approving the use of electronic surveillance in such circumstances. Petrow Interview, *supra* note 45.

Type of Entity	Approval Authority	Source(s) of Authority
All emergencies	Attorney General	50 U.S.C. § 1805(e)
Non-U.S. person	Attorney General[69]	50 U.S.C. § 1802(a); Exec. Order 12,333, § 2.5
U.S. person	FISC Judge	50 U.S.C. § 1802(b)

How Does One Obtain a FISA Court Order?

Obtaining a court order which approves electronic surveillance or physical searches for counterintelligence purposes under the FISA is primarily a legal task. This is an extraordinarily complex area of practice involving cases with potentially explosive media coverage and damage to national security. Managing a national security case is a task that no one person or agency handles alone. When determining who to call, and throughout the development of the case, judge advocates must remember that only intelligence entities can conduct counterintelligence operations. Within the Army, intelligence entities include division and corps military intelligence (MI) assets, as well as the six regionally-oriented MI brigades or groups that are part of United States Army Intelligence and Security Command (INSCOM). The Army Criminal Investigation Command has no role in conducting counterintelligence operations, including the use of electronic surveillance.[70] The intelligence agency that will commonly assist in electronic surveillance efforts, and the one that is the lead agency for all counterintelligence activities within the United States,[71] is the FBI.

The following is a recommended procedure for handling the hypothetical case described in the beginning of this article:

Step 1: Touch the Required Coordination Nodes

The installation must advise the FBI immediately of "any information, regardless of its origin, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power."[72] Following the initial report to the FBI, the statute requires consultation "with respect to all subsequent actions" which are taken to determine the source or extent of the loss of classified information.[73]

Even without specific information indicating a possible compromise of classified information to a foreign power, if the suspect is an employee or former employee of an Army intelligence component, the installation may be required to report the conduct to the Army General Counsel or Inspector General, who will in turn coordinate with the DOJ.[74] The 1995 Reporting of Crimes Memorandum outlines a detailed reporting mechanism and provides a detailed list of offenses which must be reported, even if the information pertains to non-employees. Finally, DOD policy requires the installation to report expeditiously "significant counterintelligence activities, criminal cases, and espionage activities."[75] In the context of national security cases, the reporting requirement applies to counterintelligence activities that are likely to receive publicity or to involve conduct which is or may constitute criminal espionage.[76]

68. The FISA applies to both electronic surveillance and physical searches for foreign intelligence purposes.

69. The Attorney General may elect, however, to seek FISC approval for the use of electronic surveillance within the United States involving non-U.S. persons.

70. The Army Criminal Investigation Command (CIDC) is not a DOD intelligence component. AR 381-10, *supra* note 42, at A1-2. This differs from both the Navy and Air Force, as their investigative services each possess counterintelligence elements. In certain circumstances, Army intelligence components must provide details of intelligence investigations to the CIDC. U.S. DEP'T OF ARMY, REG. 381-20, U.S. ARMY COUNTERINTELLIGENCE (CI) ACTIVITIES (15 Nov. 1993) [hereinafter AR 381-20]. In the process of seeking a FISA court order for electronic surveillance, however, judge advocates should not contact either the CIDC or the local Provost Marshal. Telephone Interview with Edward G. Allen, Command Counsel, U.S. Army Foreign Intelligence Command/902D MI Group (Dec. 11, 1996) [hereinafter Allen Interview] (notes on file with authors).

71. EO 12,333, *supra* note 3, para. 1.14(a).

72. Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 811, 108 Stat. 3455, *codified at* 50 U.S.C.A. § 402a (West 1996).

73. *Id*. If further investigation reveals that the suspect did not disclose the classified information to a foreign power but did improperly remove the classified information from the authorized storage area, the trial counsel should refer to 18 U.S.C.A. § 1924 (West 1996), which imposes a fine of up to $1,000 or one year imprisonment for removal with the intent to "retain such documents or materials at an unauthorized location."

74. EO 12,333, *supra* note 3, § 1.7(a); 1995 CRIMES REPORTING MEMORANDUM OF UNDERSTANDING BETWEEN THE DEPARTMENT OF DEFENSE AND THE DEPARTMENT OF JUSTICE (8 Sept. 1995) (copy on file with authors). *See also* 28 U.S.C.A. § 535(b) (West 1996) (requiring agencies to report violations of federal criminal laws to the Attorney General whether or not the offender is employed by an intelligence component).

75. U.S. DEP'T OF DEFENSE, INSTR. 5240.04, REPORTING OF COUNTERINTELLIGENCE AND CRIMINAL VIOLATIONS (22 Sept. 1992) (describing reportable items and outlining required reporting channels through the DOD Inspector General).

76. *Id*. para. C. The judge advocate must prepare a report describing the nature of the offense, a summary of the facts, identification of the persons involved, and a brief summary of actions taken. *Id*. In addition, cases involving counterintelligence or espionage should include a statement of the nature and sensitivity of the information involved. *Id*. para. G(5).

Step 2: Determine if the FBI has the Investigative Lead

After the 1995 Reporting of Crimes Memorandum, Congress passed the Antiterrorism and Effective Death Penalty Act of 1996.[77] The statute made it a crime to commit acts of terrorism which transcend national boundaries. The statute also gave the Attorney General "primary investigative responsibility for all federal crimes of terrorism,"[78] which are defined as offenses "calculated to influence or [to] affect the conduct of government by intimidation or coercion, or to retaliate against government conduct"[79] and which involve violations of any of the federal criminal laws that are listed in the statute.[80]

The hypothetical case at the beginning of this article does not appear to involve any of the offenses specified in the statute; therefore, the military would retain the lead. The FBI would assume the lead investigative responsibility for the investigation if later information links the suspect employee to one or more of the listed offenses (such as providing aviation information to assist terrorist groups).

Step 3: Define the "Primary Purpose" of the Investigation

At the onset of an investigation, judge advocates who seek warrants under the FISA must inform the SJA of the major command about the situation.[81] The technical channel coordination will pave the way for eventual coordination through the appropriate General Counsel offices, but the required coordination with the SJA may prove to be beneficial in many ways.

Next, judge advocates should contact the MI Group field office that is responsible for the unit or activity in which the suspected person works.[82] The MI field office will in turn relay all necessary information, including the request for the use of electronic surveillance, through company and battalion levels to the MI Group.[83] At this level, Army counterintelligence planning occurs.

The critical stage of the initiation and development of the investigation involves the clear and prompt determination of its primary purpose. As former Attorney General Griffin Bell stated, "every one of these counterintelligence investigations . . . involves crime in an incidental way. You never know when you might turn up with something you might want to prosecute."[84] From the beginning, the investigators must determine whether the investigation is primarily an intelligence effort, which will be coordinated and conducted by counterintelligence agents, or a law enforcement investigation.

To assist in the primary purpose determination, the SJA should appoint an intelligence oversight officer[85] to serve in a quasi-judicial role as an impartial mediator between competing organizational interests. At the installation level, the intelligence oversight officer should convene a counterintelligence coordination meeting between the appropriate unit commanders, the local MI assets, and the Criminal Investigation Division representatives. It is vital for the intelligence oversight officer to include the commander in the meeting. The commander will be the one deciding how to dispose of any future criminal charges, and he is able to provide input concerning the importance of immediate prosecution of the case. In addition, the commander should be involved at this stage because the development of the case as an intelligence investigation will almost certainly mean that the suspect will continue to have access to classified information, which has implications for the unit's security.

In addition to serving as a convenient local forum for the exchange of information, the counterintelligence coordination meeting has several purposes. First, the intelligence oversight officer can use the meeting to collect information which will then be relayed to the Army Central Control Office. Prior to

---

77. Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1214 (1996).

78. *Id.* § 702, *codified at* 18 U.S.C.A. § 2332b (West 1996).

79. 18 U.S.C.A. § 2332b(g)(5)(A).

80. Judge advocates should refer to the extensive list of offenses in the statute. The list includes many offenses that could conceivably be committed in areas under military control, such as: 18 U.S.C.A. §§ 32 (relating to destruction of aircraft or aircraft facilities; 81 (relating to arson within special maritime and territorial jurisdiction); 175 (relating to biological weapons); 842(m), (n) (relating to plastic explosives); 844(e) (relating to certain bombings); 1361 (relating to inury of government property or contracts); 1362 (relating to destruction of communication lines, stations, or systems); 1363 (relating to injury to buildings or property within special maritime and territorial jurisdiction of the United States); 1992, 2152 (relating to injury of fortifications, harbor defenses, or defensive sea areas); and 2155 (relating to destruction of national defense materials, premises, or utilities).

81. Office of The Judge Advocate General, U.S. Army, Policy Letter 97-4, *Use of the Technical Channel of Communications* (17 Sept. 1996).

82. In situations where the MI field office is unknown, the judge advocate can call the legal advisor for the regional MI group. The MI group legal advisor will inform all subordinate MI activities. Allen Interview, *supra* note 70.

83. *Id.*

84. United States v. Truong Dinh Hung, 629 F.2d 908, 916 n.5 (4th Cir. 1980).

85. The chief of the SJA's administrative law office would be a good choice to serve in this capacity.

formally opening an intelligence investigation, the control office must determine that the offense and personnel believed to be involved are within the Army investigative jurisdiction.[86] Second, the participants should determine the offenses which may be involved in the incident. The list of possible offenses will help determine the primary purpose of the investigation.[87]

Even though some of the alleged conduct might be identified as criminal, the intelligence interests of exploitation, damage assessment, development of an association matrix, or surveillance of foreign intelligence assets might indicate that the primary purpose for the investigation should be counterintelligence. Conversely, if the early stages of investigation eliminated the involvement of a foreign power, a primary purpose of law enforcement is logical and would require law enforcement assets and procedures. In either instance, the intelligence oversight officer should document the rational for the determination of the investigation's primary purpose.

The involvement of the intelligence oversight officer during the early stages can prevent future problems in the resolution of the case. If the case results in a court-martial which will require the use of evidence derived from FISA warrants, the trial judge will delay the trial pending a federal district court's determination of the legality of the FISA procedure.[88] Rather than forcing the trial counsel to testify, the intelligence oversight officer will be available to testify to the federal district court if necessary. In addition, insulating the trial counsel from the determination of the investigation's primary purpose helps eliminate any prosecutorial taint which might endanger subsequent judicial review of the foreign intelligence information sought under the FISA.

In the hypothetical case at the beginning of this article, as in all domestic instances, the MI Group will apprise the FBI of the developing counterintelligence situation.[89] In most instances, the FBI will assume lead agency status for domestic investigations. Several reasons support this course of action. First, Army MI jurisdiction is much narrower than the scope of criminal investigative jurisdiction; it extends only to soldiers and not to civilians.[90] Second, even in situations where Army MI jurisdiction exists, the FBI's greater experience favors its primary role. Third, the more byzantine procedures within the military approval process for electronic surveillance applications make the FBI a preferred choice in time sensitive situations.

Step 4: Coordinate the FISA Application Process

In instances where the Army retains jurisdiction for a counterintelligence activity, a request for authority to conduct electronic surveillance or to conduct a physical search for an intelligence purpose must pass through many hands. The application goes from the MI Group to the INSCOM.[91] The INSCOM will provide notice of the counterintelligence matter to the Deputy Chief of Staff for Intelligence and will forward the developing FISA application to the Office of the Army General Counsel. After legal review and approval, the request for electronic surveillance goes to the DOD General Counsel's Office for review. The DOD General Counsel will then seek approval and the necessary executive branch certification from the Secretary of Defense, the Deputy Secretary of Defense, the Secretary of the Army, or the Under Secretary of the Army.

From the DOD General Counsel's Office, the FISA application must go to the DOJ. The Office of Intelligence Policy and Review (OIPR)[92] is the section responsible for rewriting and assembling the electronic surveillance application to ensure that it contains all of the elements and certifications required by statute. The completed application goes from the OIPR to the Attorney General for final review and signature. An attorney from the OIPR will then take the completed product to one of the FISC judges for review and approval.[93]

When the FBI is the lead agency for a counterintelligence activity, an application under the FISA has a different route for approval. The counterintelligence section of the FBI field office develops the facts of the case. An FBI counterintelli-

86. AR 381-20, *supra* note 70, para. 4-2f.

87. *Id*. para. 4-5. The CID has the investigative lead for actual or suspected instances of sabotage. *Id*.; U.S. DEP'T OF ARMY, FIELD MANUAL 34-60, COUNTERINTELLIGENCE D-4 (5 Feb. 1990).

88. *See supra* note 16.

89. Allen Interview, *supra* note 70.

90. Judge advocates may, in situations involving civilians, elect to call directly the local FBI senior resident agent, who will then contact the counterintelligence section of the nearest large office. The FBI is required to coordinate with the various defense departments when the counterintelligence activity involves DOD personnel. EO 12,333, *supra* note 3, § 1.14(a). Judge advocates should still inform the MI Group legal advisor about such situations. Allen Interview, *supra* note 70.

91. Allen Interview, *supra* note 70.

92. The OIPR not only reviews FISA applications at the end of the process, but also will provide advice and consultation to the legal advisors of counterintelligence agencies during the process. The primary point of contact for electronic surveillance operations and application requests is Allan Kornblum, Deputy Counsel for Intelligence Operations. Mr. Kornblum's phone number is (202) 514-2882. Petrow Interview, *supra* note 45.

93. A FISA court judge or the court's legal advisor can let the OIPR know if they see a problem with an application. The government can then withdraw or amend the application. MCGEE & DUFFY, *supra* note 15, at 318.

gence supervisory agent, located at the headquarters level, is responsible for developing the facts to support the FISA application. The FBI General Counsel's Office will then review the application and obtain the approval and certification of the Director of the FBI. Afterwards, the OIPR will prepare the final electronic surveillance application to ensure that it meets all statutory requirements. The Attorney General is the final review and approval authority before presentation to a FISC judge. This process can be very speedy if the installation works with the FBI to ensure that the application contains the most accurate and statutorily required information. In any case, the lawyers processing FISA applications will not know about pressing investigative circumstances unless the agents and lawyers from the field communicate their requirements.

Conclusion

The intelligence agencies of the United States are responsible for providing "timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers and their agents."[94] Military attorneys are responsible for providing timely and accurate legal advice to ensure that military intelligence activities can protect the national security of the United States while abiding by the statutory and regulatory frameworks which preserve civil liberties.

In the area of electronic surveillance, judge advocates must analyze three key aspects in each situation: purpose, approval authority, and process. They must ensure that the purpose for the desired collection of information is primarily one of counterintelligence and not law enforcement;[95] know the approval authority required for various situations, including some where the approval authority lies outside of the DOD; and know how to make the process work for, and not against, them. This will often mean that the military attorney serves as a conduit of legally defensible and factually correct information to support the certifications which support subsequent FISA warrants. An intellectual appreciation of the philosophical underpinnings of the law is little solace, for both lawyer and client, if the investigative process fails to preserve national security and allows criminals to remain unpunished. By providing timely and accurate information on these three aspects, Army lawyers can do their part to further the intelligence efforts of the United States while serving the ends of justice.

94. EO 12,333, *supra* note 3.

95. The FISA assists in this endeavor by requiring executive branch officials to articulate the rationale for planned activities. *See* Mary C. Lawton, *Review and Accountability in the United States Intelligence Community,* OPTIMUM: J. PUB. SEC. MGMT., at 101-02 (Autumn 1993).