FISA/Info Sharing > FISA Recipe

"What do I have to do to get a FISA?"

Introduction

This discussion of the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801 et seq., ("FISA", or "the statute") provides guidance for seeking authorization to conduct electronic surveillance or physical searches for foreign intelligence purposes. In response to the basic question, "What do I have to do to get a FISA?," first, step back and take a look at the big picture. FISA was enacted to provide a statutory procedure for the government to obtain court orders authorizing the use of electronic surveillance in the United States for foreign intelligence purposes. Later, section 807 of the Intelligence Authorization Act for Fiscal Year 1995 (P.L. 103-359) amended FISA to authorize the Court to issue warrants for *physical searches* for foreign intelligence purposes. Accordingly, FISA deals with electronic surveillance and physical searches of foreign powers and their agents. If your purpose is other than the acquisition of foreign intelligence information, as defined by the statute, you're probably in the wrong forum.

Without going into the historical background of FISA in detail, the impetus for its enactment was largely concern for the privacy rights of U.S. persons, balanced against the government's need to obtain foreign intelligence information . As a result, the statute's treatment of "U.S. persons" and "non-U.S. persons" is different. For example, in considering this legislation, Congress stated that a U.S. person should be confident that his government cannot invade his privacy with the most intrusive techniques if he conducts himself lawfully and that, as a matter of public policy, no U.S. person should be targeted for electronic surveillance [or physical search] absent some showing that he at least "may" violate the law. On the other hand, surveillance pursuant to FISA is not primarily for the purpose of gathering evidence of a crime, although evidence of a crime may well be acquired in surveilling persons who engage in the types of activities that define them as agents of foreign powers. As a result, FISA explicitly recognizes that evidence of a crime may be acquired in the course of surveillance or search conducted to protect the United States from the clandestine intelligence activities and international terrorist activities of foreign powers and their agents. Prosecution for a criminal offense is one way to combat such activities -- but only one way, and not always the best way. "Doubling" an agent or feeding him false or useless information are other ways. Monitoring him to discover other agents and their tradecraft can be vitally useful. Prosecution, while disabling one known agent, may only mean that the foreign power replaces him with one whom it may take years to discover or who may never be discovered.

With regard to non-U.S. persons who act in the United States in their official capacities, or who are members of international terrorist groups, however, no nexus to criminality is required, and they are defined as agents of foreign powers solely on the basis of their status. In addition, the retention and dissemination of information concerning non-U.S. persons is signficantly less regulated that that of U.S. person information.

The FISA Court

FISA authorizes the government to apply to a special "Foreign Intelligence Surveillance Court" ("FISC" or "FISA court") for an order approving the use of electronic surveillance or physical search to acquire foreign intelligence information. Pursuant to an October, 2001, amendment by the USA PATRIOT Act, the FISA Court is composed of eleven judges designated by the Chief Justice of the United States. Historically, the judges were chosen from different circuits, but the amendment increasing the number of judges from seven to eleven also specified that they come from seven of the judicial circuits and that no fewer than three shall reside within 20 miles of the District of Columbia.

Approval of a FISA application requires a finding by the court that there is probable cause to believe that the

63

target of the proposed surveillance is a "foreign power" or a [illegible]ent of a foreign power," and that the facilities or places at which the surveillance is directed are used or are about to be used by that foreign power or agent of a foreign power. In addition to determining whether there is probable cause to support the application, the Court is also required to find that procedures proposed in the application to regulate the acquisition, retention and dissemination of information concerning U.S. persons meet the definition of "minimization procedures " in section 101(h) of the statute. Because the showing that the target of the proposed surveillance or search is a "foreign power" or an "agent of a foreign power," the definitions of these terms are particularly important. Other terms are also important, including "international terrorism," "foreign intelligence information," "electronic surveillance," "physical search" and "United States person," all of which are defined in section 101 or 301 of the statute and will be discussed in detail, *infra*.

Subsection 105(a) of FISA specifies the findings the court must make before he grants an order approving the use of electronic surveillance for foreign intelligence purposes. While the issuance of an order is mandatory if the court finds that all of the requirements of this section are met, the judge has the discretionary power to modify the order sought, such as with regard to the period of authorization or the minimization procedures to be followed. In practice, the FISA Court has found general supervisory powers in this language, and its power to modify minimization procedures has been used as power to influence or control other aspects of investigations. This is essentially what the Court did in its April 22 and May 17 orders in construing discussions between intelligence officials and law enforcement officials about investigative strategies and tactics as "minimization procedures" that required OIPR attendance to ensure that such discussions did not result in and in requiring OIPR be invited to attend.

Probable Cause . . .

In general terms, FISA deals with "foreign powers" and "agents of foreign powers," and the fundamental requirement for the Court's granting a FISA application is probable cause to believe that the proposed subject of surveillance or search is a foreign power or an agent thereof. "Foreign power" includes a foreign government; a faction of a foreign government; a group engaged in international terrorism; a foreign-based political organization; or an entity directed and controlled by a foreign government or governments. An "agent of a foreign power" includes non-resident aliens who act in the United States as officers, members or employees of foreign powers, or who act on behalf of foreign powers that engage in clandestine intelligence activities in the United States contrary to the interests of this country. U.S. persons meet the "agent of a foreign power" criteria if they engage in certain activities for or on behalf of a foreign power which involve, or may involve, certain criminal acts.

Subsection 105(a)(3) provides that in order to issue an order for electronic surveillance, the Court must find that on the basis of the facts submitted by the applicant there is "probable cause" to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power and that each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. Subsection 304(a)(3) provides for similar findings with regard to physical search. As to both electronic surveillance and physical searches, no United States person may be considered a foreign power or an agent of a foreign power solely on the basis of activities protected by the First Amendment to the Constitution.

Probable cause in the FISA context is similar to, but not the same as, probable cause in criminal cases. Where a U.S. person is believed to be an agent of a foreign power, there must be probable cause to believe that he is engaged in certain activities, for or on behalf of a foreign power, which activities involve or may involve a violation of U.S. criminal law. The phrase "involve or may involve" indicates that the showing of [nexus to] criminality does not apply to FISA applications in the same way it does to ordinary criminal cases. As a result, there is no showing or finding that a crime has been or is being committed, as in the case of a search or seizure for law enforcement purposes. The activity identified by the government in the FISA context may not yet involve criminality, but if a reasonable person would believe that such activity is likely to lead to illegal activities, that would suffice. In addition, and with respect to the nexus to criminality required by the definitions of "agent of a foreign power," the government need not show probable cause as to each and every element of the crime involved or about to be involved.

The determination as to probable cause to believe that a target is engaging in certain activities, or that an entity is directed and controlled by a foreign government, should take into account the same aspects of reliability of the government's information as in the ordinary criminal context, including the reliability of any informant, the circumstances of the informant's knowledge and the age of the information relied upon. On the other hand, not all of the same strictures with respect to these matters which have developed in the criminal context may be

64

appropriate in the foreign intelligence context. That is, in the criminal context certain rules have developed or may develop for judging reliability of information. FISA does not require that the "rules" necessarily be applied to the probable cause determination. Rather, in judging the reliability of the information presented by the government, look to the totality of the information and consider its reliability on a case-by-case basis.

In *Illinois v. Gates*, 462 U.S. 213 (1983), the Supreme Court overruled rigid application of the two-pronged test for the reliability of an informant set forth in *Spinelli v United States*, 393 U.S. 410 (1969). *Spinelli* required both knowledge of the source of an informant's information as well as information as to the reliability of a source before his information could used to establish probable cause. *Gates* acknowledged that it was appropriate to consider such factors as instructive, but they should not be applied with mathematical precision. As a result, *Gates* stands for a "totality-of-the-circumstances" approach.

Also instructive is the case of *Brinegar v. United States*, 338 U.S. 160 (1949), which noted that probable cause is a factual and practical consideration of everyday life on which reasonable and prudent men act, not legal technicians. At the same time, probable cause is based on a presentation of reliable and corroborated facts, not mere suspicion.

Simply put, "probable cause" is reason to believe, based on available facts and circumstances, as well as the logical inferences that can be drawn from them. It is determined by the totality of the facts and circumstances, as viewed from the perspective of a reasonable person. Probable cause probability, not certainty, and, thus, is significantly lower than the "proof beyond a reasonable doubt" necessary to support a criminal conviction. It is also lower than the "preponderance of the evidence" required in most civil cases.

NSLU recommends that a field agent seeking a FISA order focus on the *object* of the belief required, *i.e.*, the facts and circumstances demonstrating that the target of the proposed search or surveillance is an agent of a foreign power and that the premises to be surveilled (*e.g.*, telephone) is used by that agent of a foreign power, rather than on the *quantum* of the belief involved. If you can show that a target is engaged in certain activities, and that he is engaged in them for or on behalf of a foreign power, you have won most of the battle.

No U.S. person may be considered an agent of a foreign power based solely on activities protected by the First Amendment to the Constitution. This provision is intended to reinforce the congressional intent that lawful political activities should never be the sole basis for a finding that a U.S. person is a foreign power or an agent thereof. For example, under the Supreme Court's decision in *Brandenburg v. Ohio*, 395 U.S. 444 (1969), the advocacy of violence, falling short of inciting violence, is protected by the First Amendment. Thus, advocating the commission of terrorist acts would not, in and of itself, be sufficient to establish probable cause to believe that an individual or group may be preparing to commit such acts. However, one cannot cloak himself in First Amendment immunity where he is engaged in clandestine intelligence activities, terrorism or sabotage. ["The Constitution is not a suicide pact."]

. . . Probable Cause to Believe What?

To find probable cause to believe the subject of the surveillance is an "agent of a foreign power," as defined in subsection 101(b), the court must find that each and every element of that status exists. If a U.S. person is alleged to be acting on behalf of a foreign entity, the court must first find probable cause to believe that that entity is a "foreign power," as defined in subsection 101(a). There must also be probable cause to believe that the person is acting "for or on behalf of" that foreign power, as well as probable cause to believe that the efforts undertaken by the target on behalf of the foreign power constitute sabotage, international terrorism or clandestine intelligence activities. Similar findings are required for each element necessary to establish that a U.S. person is conspiring with or aiding and abetting someone engaged in sabotage, international terrorism or clandestine intelligence activities.

The Theory of the Case

The development of a "theory of the case" is a good start to the FISA process. That is, before asking FBIHQ for initiation of an application to the FISA Court, the field agent should review the facts of the case to determine which definition of "foreign power" and/or "agent of a foreign power" best matches the information obtained by the investigation to date. For example, if the subject is a U.S. person who is believed to be knowingly

65

engaged in aiding and abetting an international terrorist, focus on facts that show his activities that aid a terrorist, as well as on facts that tend to demonstrate his knowledge that the person he is aiding is an international terrorist and that his activities aid that international terrorist. If the subject is a non-U.S. person who acts in the U.S. as an employee of a foreign government, focus on presenting facts that demonstrate that status. In such a case, a recitation of intelligence activities is not as important as it would be in the case of a U.S. person, as to whom the FBI would have to show facts demonstrating knowing engagement in clandestine intelligence activities.

It is also helpful to articulate the specific foreign intelligence objectives of the proposed surveillance or search. In an espionage case, *e.g.*, your objective may be to determine whom an intelligence officer has targeted for recruitment. Or you may need to know how a government employee is communicating with an intelligence officer who is his handler. Or you may need to determine the identity of a foreign power a spy is working for, how he obtains access to classified information, whether he is working alone or in concert with others and how he passes information to his handler. In an international terrorism case, your objectives may include identifying the members of the terrorist group or identifying their plans and intentions in order to prevent a terrorist attack.

§ 101(b) -- Agent of a foreign power

Probably the single most important aspect of the request for a FISA application is showing that the subject to be surveilled or searched is an "agent of a foreign power." The definitions of "agent of a foreign power" differ for U.S. persons and certain non-resident aliens, including aliens present in the United States as tourists, visiting businessmen, exchange visitors, foreign seamen, diplomatic and consular personnel and illegal aliens, etc. The protections afforded such persons are not as great as those afforded U.S. persons. For example, in the case of non-resident aliens who are agents of foreign powers by virtue of their employment in the U.S. by a foreign government, there need be no nexus to criminality, and the certification that accompanies the application is not subject to judicial review. In addition, there is no requirement to minimize the acquisition, retention and dissemination of information with respect to non-U.S. persons.

§ 101(b)(1) -- Non-U.S. Persons Who Are Agents of a Foreign Power by Virtue of Status

Subsection 101(b)(1)(A) includes in its definition of "agent of a foreign power" non-U.S. persons who act in the United States as officers, employees or members of a foreign power. The most obvious examples are diplomats and consular officials. Their very presence is attributable to their status as employees of their governments, and their *raison d'etre* is to act for or on behalf their governments. The legislative history of FISA points out that Congress considers non-resident aliens who act in the United States as officers, employees or members of a foreign power as likely sources of foreign intelligence or counterintelligence information. This definition does not include persons who serve as officers or employees or are members of a foreign power in their home country, but who do not act in that capacity in the United States.

"Employee" is meant to describe a normal employee-employer relationship. It does not encompass foreign visitors such as professors, lecturers, exchange students, performers or athletes, even if in such capacity they are receiving remuneration or expenses from their home government.

The term "member" means an active, knowing member of a group or organization that is a foreign power. It does not include mere sympathizers, fellow-travelers or persons who have merely attended meetings of the group or organization. On the other hand, if a person has received terrorist training from a group engaged in international terrorism or training in intelligence tradecraft from a foreign organization, this would be substantial evidence that he was a "member" of such an entity.

Unlike foreign officials, members of international terrorist groups do not carry membership cards as evidence of their status. They do not have visas or credentials identifying them as "members" of an IT group or organization. As a result, their status as members of a group or organization engaged in international terrorism is inferred from their activities.

The second non-U.S. person definition is the so-called "visitor rule." It includes a non-U.S. person who --

> acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in

the United States, or when such person knowingly aids or abets any person in the ... uct of such activities or knowingly conspires with any person to engaged in such activities.

This definition does not require a showing that the foreign visitor is in fact engaged in clandestine intelligence activities. As a practical matter, if a foreign visitor who does not have a track record of activities in the United States is present in the U.S. for only a limited period of time, and the FBI is limited to the use of less intrusive techniques, the FBI is not likely to be able to show that he is actually engaged in intelligence or terrorist activities. He can be characterized as an agent of a foreign power, however, if it can be shown that the foreign power on whose behalf he acts systematically engages in clandestine intelligence [or terrorist] activities that threaten the security of the United States. It is a demonstration based on *probability; i.e.*, it is not a showing that the individual foreign visitor is himself currently engaged in clandestine intelligence activities, but that the *circumstances* of his presence in the U.S. indicate he *may* engage in such activities because the foreign power for whom or on whose behalf he acts has demonstrated some pattern or practice of engaging in clandestine intelligence activities in the United States contrary to U.S. interests.

The phrase "acts for or on behalf of a foreign power" requires a nexus between the individual and the foreign power that suggests that he is likely to do the bidding of the foreign power. For example, visitors from totalitarian countries present in the United States under the auspices, sponsorship or direction of their government would satisfy this standard.

Once the requisite facts with regard to the foreign power are established, the key question is whether the circumstances of the person's presence in the U.S. indicate that he may engage in clandestine intelligence activities for that foreign power contrary to U.S. interests. The answer may vary according to what is known about the intelligence or terrorist operations of the particular foreign power. Among the factors that might be taken into account are whether the foreign visitor engages in activities with respect to which there is evidence that other visitors who engage in similar activities are officers, agents or acting on behalf of the intelligence service of that foreign power. If the FBI can show from experience that a particular foreign power uses a certain class of visitors to this country for carrying out secret intelligence assignments, this would indicate that other visitors in this class may also engage in clandestine intelligence activities.

"May engage in such activities" means that surveillance can be conducted to *anticipate* clandestine intelligence activities by such persons, rather than waiting until they have taken place. The additional standards for aiding and abetting, and conspiracy, require probable cause to believe that the foreign visitor is knowingly assisting persons who are already engaged in clandestine intelligence activities. The "knowing" requirements are the same as in the aiding or abetting and conspiracy standard for U.S. persons.

This provision does *not* treat nationals of certain countries differently from others solely on the basis of nationality, and it is *not* "profiling." Instead, surveillance of the nationals of certain countries depends on the *activities* of the governments of those countries and whether the individual is *acting on behalf of* the government.

"Any Person" Agent of a Foreign Power

§ 101(b)(2)(A) -- Clandestine Intelligence Gathering Activities

Under this definition, an agent of a foreign power is "any person who is knowingly engaged in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal laws of the United States."

The first aspect of this definition is that the subject is engaging in certain activities "knowingly." This does not mean that he must know that he may be violating a particular federal criminal statute, but that he knows that what he is doing is clandestine intelligence gathering activities and that he knows that he is doing it for or on behalf of a foreign power. As state of mind is always difficult to show, knowledge is inferred from the circumstances. In showing that a person is knowingly engaged in clandestine intelligence gathering activities, focus on his *activities*. If, for example, a subject is transmitting classified defense secrets to the military attache of a foreign embassy, and he knows the information is classified and that his recipient is a military attache, this would be sufficient to show that he "knows" that he is acting for or on behalf of a foreign power. Similarly, if he has received training in the use of equipment for espionage, *e.g.*, a microdot camera or disguised radio device, this would be sufficient to show that he "knows" what he is doing. One who is unwitting to what he is doing, or

without knowledge that he is acting for or on behalf of a foreign power, is not an agent of a foreign power, but the government is not required to prove ignorance if a person engaging in such activities would reasonably have known that he was acting for or on behalf of a foreign power.

Next, the person must be "engaged" in the proscribed activities. Unlike the standard for foreign visitors, the fact that he "may engage" in such activities some time in the future is not sufficient. For example, if information shows that a person has recently engaged in such activities, this would normally suffice to show probable cause that he is "engaged." On the other hand, information that a person engaged in the prohibited activities in the past might well, depending on the circumstances, be sufficient to show probable cause to believe that he is still engaged in such activities. For example, information that a U.S. person was for years a spy for a foreign power hostile to the United States, but who had dropped out of sight for a few years, would probably be sufficient to show "probable cause" that he was, having now reappeared, continuing to engage in the clandestine intelligence activities.

Perhaps the most important element of this definition is "clandestine intelligence gathering activities." Most clandestine intelligence gathering activities will constitute a violation of the various federal criminal laws aimed at espionage either directly or by failure to register (see, *e.g.*, 18 U.S.C. §§ 792-799, 951; 42 U.S.C. §§ 2272-2278b; and 50 U.S.C. § 855). The term "clandestine intelligence gathering activities" is intended to mean "espionage" in common parlance; it is not a legal term of art denoting a particular offense. The term also includes activities that are directly supportive of espionage, such as maintaining a "safehouse," servicing "letter drops," running an "accommodation address," laundering funds, recruiting new agents, infiltrating or exfiltrating agents under cover, creating false documents for an agent's "cover" or utilizing a radio to receive or transmit instructions or information by "burst transmission." The term "clandestine intelligence gathering activities" is intended to mean activities in which no reasonable person would engage without knowing that society would not condone it.

As the words indicate, the activities must be "clandestine," *i.e.*, the subject must have made some efforts to conceal his activities. This does not necessarily mean that the information gathered by the agent must itself be secret or nonpublic, although this is usually the case. It is possible that a person might be asked to obtain information that is publicly available, but which a foreign power would not want known it was seeking. If he used false identification or ruse to obtain the information and then delivered the information by means of a microdot hidden in a magazine left at a "dead drop," both the means by which he gathered the information and the means by which he transmitted it would be "clandestine," even though the information itself might not be secret. The FBI may surveil such a person, even if the information he is collecting is not classified, because his activities identify him as an agent of a foreign power. By monitoring his contacts, their equipment and *modus operandi*, the FBI can learn valuable information concerning the tactics, capabilities and personnel of the foreign intelligence service.

"Clandestine intelligence gathering activities" are intended to be conduct of a nature associated with spies and espionage in its generic sense, but the term is supposed to be flexible with respect to what is being gathered because intelligence priorities and requirements differ between nations and over time. Obviously, gathering classified defense information, information about intelligence sources and methods and classified foreign relations information qualifies as "clandestine intelligence gathering activities" if it is done in a clandestine manner. Foreign powers also target American technology and trade secrets, economic developments, political information and even personal information for purposes of blackmail or other coercion, so that attempts to collect such information may also be "clandestine intelligence gathering activities."

It is possible, although unlikely, that some people might come close to using espionage techniques for otherwise lawful purposes. Thus, the definition requires that the person be engaged in clandestine intelligence gathering activities "for or on behalf of a foreign power." The fact that a person gathers information and transmits it to a foreign power does not, by itself, satisfy the requirements of this definition, as people may legitimately gather information for foreign powers. Registered lobbyists, *e.g.*, often do, but their activity, if legitimate, does not utilize the tradecraft of espionage or clandestine methods, to do so. This means that the FBI must show probable cause to believe that the person is not only engaged in clandestine intelligence gathering activities, but that he is doing so for or on behalf of a foreign power. Thus, showing that a person is stealing defense secrets and using a "dead drop" to pass them on is not enough; it must be shown that he is doing so for a foreign power.

The FBI must show that there is probable cause to believe that a subject is engaged in activity that at least "may" violate a federal criminal statute. As noted above, it is expected that most persons under this definition would be likely to violate laws directed against espionage. There are other laws, however, that might be violated,

68

such as interstate transportation of stolen property or the Export Administration Act. The crime involved might be one of several violations depending, for example, upon the nature of the information being gathered.

The words "may involve" are intended to encompass clandestine intelligence gathering activities that may, as an integral part of such activities, involve a violation of federal law. They cover the situation in which the FBI cannot establish probable cause to believe that a foreign agent's activities involve a specific criminal act, but where there are specific and articulable facts to indicate that a crime may be involved. The circumstances might be such as to indicate that the activity may involve a crime. The term "may involve" requires only limited information regarding the crime involved, such that electronic surveillance may be permissible at some point prior to the time a crime, *e.g.*, the passage of classified documents, actually occurs. There need not be a current or imminent violation of law if there is probable cause to believe that criminal acts may be committed.

In applying this standard, the FISA Court takes all the known relevant circumstances into account, *e.g.*, who the subject is, where he is employed, whether he has access to classified or other sensitive information, the nature of clandestine meetings or other clandestine activity, the method of transmission and whether there are innocent explanations for the behavior. The circumstances must not merely be suspicious, but must be of such a nature to lead a reasonable man to conclude that the activity may involve a federal criminal violation.

Again, a nexus to a foreign power is absolutely necessary. Surveillance would not be authorized against a reporter merely because he gathers information for publication in a newspaper, even if the information were classified. Nor would it be authorized against a government employee who reveals secrets to a reporter or in a book for the purpose of informing the public. This definition would not authorize surveillance of ethnic Americans who lawfully gather political information and perhaps even lawfully share it with the foreign government of their national origin. Nor would it apply to lawful activities to lobby, influence or inform members of Congress or the Administration to take certain positions with respect to foreign or domestic concerns. Nor would it apply to lawful gathering of information prepatory to such lawful activities. It is the combination of (1) obtaining in clandestine fashion (2) information that is necessary to the defense or security of the United States (3) for or on behalf of a foreign power that makes FISA surveillance

In the case of an organization whose leaders are engaged in clandestine intelligence gathering activities, such activity cannot necessarily be attributed to every member of the group. There must be probable cause to believe that a particular member is himself engaged in such activity before electronic surveillance targeted against him may be authorized.

Because the standard under this definition requires that a person knowingly engage in activities for or on behalf of a foreign power, problems can arise in a situation in which a person is "turned" or "doubled," *i.e.*, after having started out as an agent for a foreign power, he is persuaded to work for the United States. The standard is not met if the person is in fact working for the U.S. and not for the foreign power. There may be doubt, however, as to whether he is actually under U.S. control or that of a foreign power, making it unclear as to which side is deceiving which. The fact that a supposedly "doubled" agent carries out his assignments and instructions from the U.S. Government does not necessarily mean that he has stopped carrying out those of the foreign power. It is not necessary, therefore, that a surveillance, once authorized, be discontinued when the agent may have been "doubled." Rather, surveillance may continue until such time as the "doubled" agent is trusted enough to seek his consent to surveillance.

§ 101(b)(2)(B) -- "Other Clandestine Intelligence Activities"

Subsection 101(b)(2)(B) defines agent of a foreign power as a person who pursuant to the direction of an intelligence service or network of a foreign power knowingly engages in "other clandestine intelligence activities" for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States. ["Other" refers to other than clandestine intelligence *gathering* activities.]

The term refers to covert actions by intelligence services of foreign powers. Not only do foreign powers engage in spying in the United States to obtain information, they also engage in activities that are intended to harm U.S. security by affecting the course of government, the course of public opinion or the activities of individuals. Such activities may include political action (recruiting, bribery or influencing public officials to act in favor of the foreign power), disguised propaganda (including the planting of false or misleading articles or stories) and harassment, intimidation or even assassination of individuals who oppose the foreign power. Such activity can undermine democratic institutions as well as directly threaten the peace and safety of U.S. citizens.

69

There may be a narrow line between clandestine intelligence activities and lawful activities undertaken by U.S. persons in the exercise of First Amendment rights. To avoid crossing that line, this definition requires that the person be shown to be acting "pursuant to the direction of an intelligence service or network of a foreign power." [No such showing is required for the other definitions of agent of a foreign power.] U.S. persons may well communicate with a foreign government to obtain information about that government's country or to discuss travel to that country, but such contacts are not necessarily "clandestine intelligence activities" and are not covered by this definition.

The activities engaged in must involve, or be about to involve, a violation of federal criminal law. This is higher than the "may" involve standard found in other definitions. In this area, where there is a narrow line between protected First Amendment activity and the activity giving rise to surveillance, it is important that the activity be such that it involves or is about to involve a violation of a federal criminal statute.

There are a number of crimes that might be involved in covert action, *e.g.*, bribery of public officials, campaign law violations, foreign agent registration requirements, denial of civil rights, *et cetera*. It is important to note, however, that such a criminal violation does not necessarily establish that a person is engaged in "other clandestine intelligence activity." Americans, through ignorance or inadvertence, may well technically violate campaign law requirements or foreign agent registration requirements, but to satisfy the requirements of the definition, it is necessary to show, separately from the criminal violation, probable cause to believe that the person is knowingly engaged in any other clandestine intelligence activities for or on behalf of such foreign power, *pursuant to the direction of an intelligence service or network of a foreign power.*

§ 101(b)(2)(C) -- Sabotage or Terrorism

Subsection 101(b)(2)(C) allows electronic surveillance or physical search of any person, including a U.S. person, who knowingly engages in sabotage or international terrorism, or activities in preparation therefor, for or on behalf of a foreign power. The terms "sabotage" and "international terrorism" are defined separately and require a showing of criminal activity. Mere sympathy for, identity of interest with or vocal support for the goals of a foreign group, even a foreign-based terrorist group, is not sufficient to justify surveillance under this subparagraph. The term "activities that are in preparation [for]" sabotage or international terrorism is intended to encompass activities supportive of acts of serious violence -- for example, purchase or surreptitious importation into the United States of explosives, planning for assassinations or financing of or training for such activities. Other activities supportive of terrorist acts could likewise satisfy this standard. The circumstances must be such as would lead a reasonable person to conclude that the subject is knowingly engaged in activities that are in preparation for sabotage or terrorism.

The term "preparation" does not mean preparation for a specific terrorist act. Because the definition of "international terrorism" speaks of a range of acts, and "preparation" as used here takes its meaning from the context of the definition of "international terrorism," it could reasonably be interpreted to include, *e.g.*, providing the personnel, training, funding or other means for the commission of acts of terrorism, rather than participating in a particular bombing. This provision also permits electronic surveillance or physical search at a time *before* the danger sought to be prevented -- whether a kidnaping, bombing or hijacking -- actually occurs.

The "preparation" standard allows surveillance where the government cannot establish that an individual has already knowingly engaged in an act of sabotage or terrorism, but there are sufficient specific and articulable facts to indicate that his activities are in preparation for such acts. The circumstances must be such as would lead a reasonable person to conclude that the subject is knowingly engaged in activities that are in preparation for sabotage or terrorism.

It should be noted that the "preparation" standard need apply only where there is insufficient information to show that the subject is, in fact, a terrorist. Where the FBI can show that the subject is a known international terrorist, such as the notorious "Carlos," or that he has been engaging in international terrorism for or on behalf of a group engaged in international terrorism, there is no need to show that he is in the act of preparing for further terrorist acts. In some cases, immediate arrest may not be possible, such as situations in which the subject may not have violated U.S. law, even though he may have murdered hundreds of persons abroad. In other cases it may be more fruitful to monitor the subject's activities in the United States to identify otherwise unknown terrorists located here, their international support structure and the locations of weapons or explosives. If a person who has engaged in international terrorism visits the U.S. or resides in the U.S., the FBI should be able to utilize electronic surveillance to monitor his activities, whether or not there is information showing that he is presently

planning some particular violent act.

Finally, a subject targeted for surveillance under this definition must be shown to have a knowing connection with the foreign power for whom he is working. In most cases of international terrorism, this connection will be shown to exist with a group engaged in international terrorism. The case may arise in which a U.S. person is acting for or on behalf of such a group that is substantially composed of U.S. persons. In such a case, the Court must examine the circumstances carefully in order to determine whether the organization is "a group engaged in international terrorism," as defined, and not a purely domestic group engaged in domestic terrorism. [Domestic terrorism is handled under criminal law processes, *e.g.*, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Title 18, U.S. Code, chapter 119, and the AG Guidelines for General Crimes.]

§101(b)(2)(D) -- Entering the U.S. under a False or Fraudulent Identity

This definition includes any person who knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power. The most obvious example would be the "illegal" who enters the United States under an assumed name and using a "legend" based on the vital statistics of a real person, usually dead. It would also include a person who enters the United States lawfully, then assumes a false identity, provided assuming such a false identity is done for or on behalf of a foreign power.

§101(b)(2)(E) -- Aiding, Abetting and Conspiracy

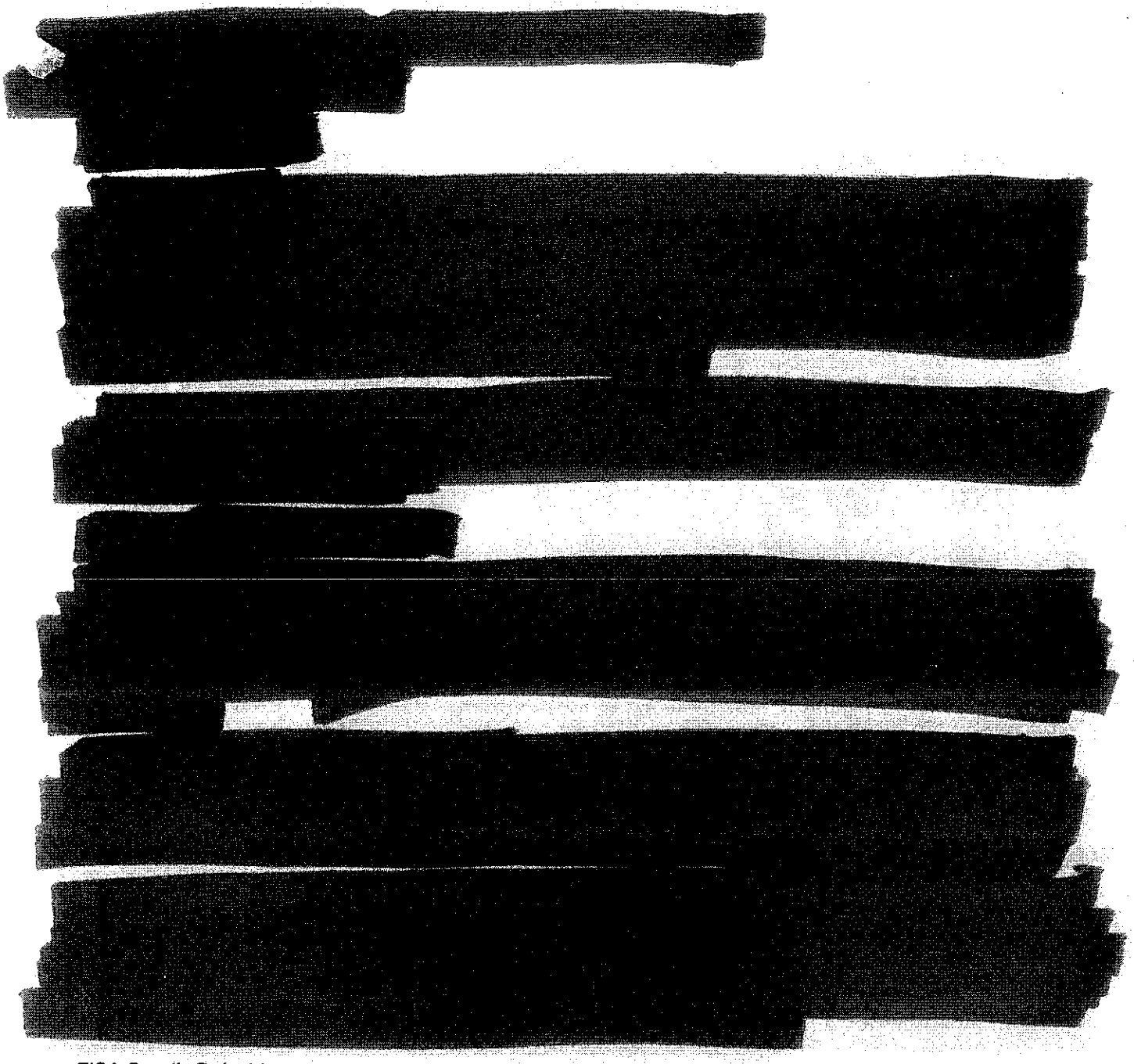
This definition includes any person, including a U.S. person, who knowingly aids or abets any person in the conduct of activities described in the preceding subsections, or knowingly conspires with any person to engage in such activities. The knowledge requirement is applicable to both the status of the person being aided and the nature of the activity being promoted. This means the FBI must establish probable cause to believe that the subject knows both that the person with whom he is conspiring or whom he is aiding or abetting is engaged in the described activities as an agent of a foreign power and that his own conduct is assisting or furthering such activities. The innocent dupe who unwittingly aids a foreign intelligence officer cannot be targeted under this provision.

In the case of a subject believed to be aiding or abetting persons engaged in international terrorism, the subject might be assisting a group engaged in both lawful political activity and unlawful terrorist acts. In such a case, it would be necessary to establish probable cause to believe that he was aware of the terrorist activities undertaken by the group and was knowingly furthering them, not merely that he was aware of and furthering the group's lawful activity.

Verification Procedures

[redacted]

b5-1
b2-2 b7E-1



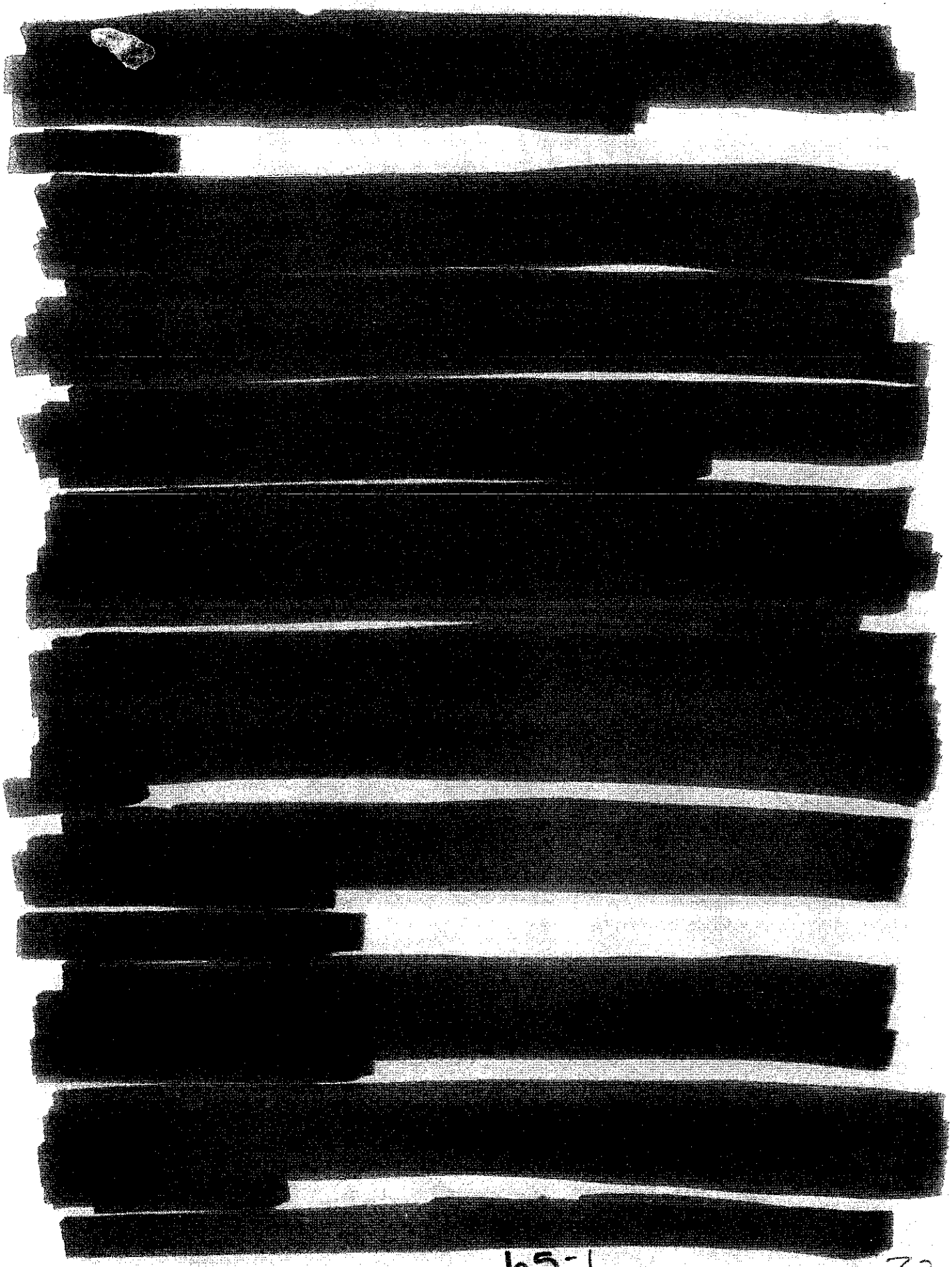
FISA Court's Rule 11

By order dated May 17, 2002, the FISA Court promulgated "Rule 11, Criminal Investigations in FISA Cases":

> All FISA applications shall include informative descriptions of any ongoing criminal investigations of FISA targets, as well as the substance of any consultations between the FBI and criminal prosecutors at the Department of Justice or a United States Attorney's Office.

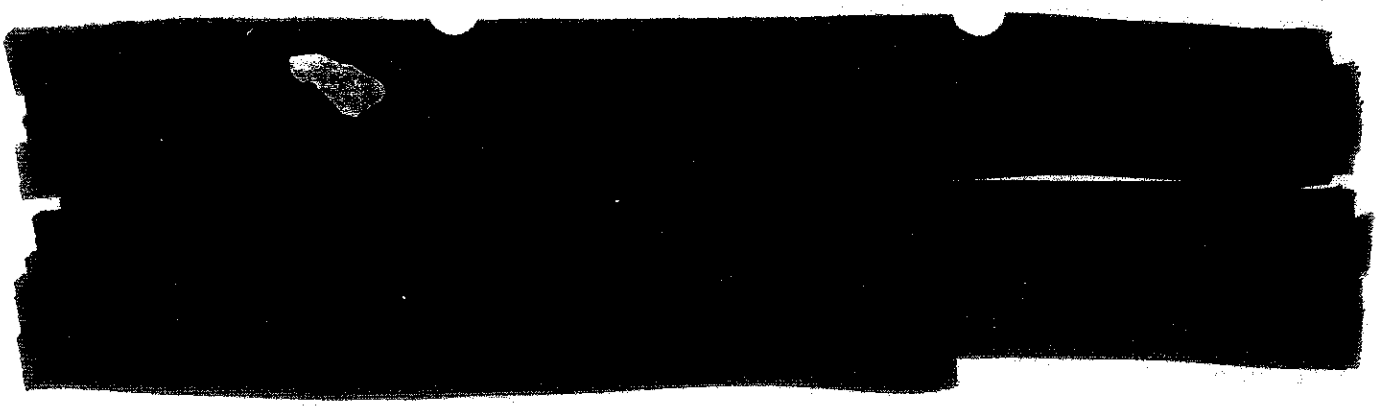
Rule 11 formalizes the requirement for descriptions of any ongoing criminal investigation, an issue that was addressed in the "verification procedures" dated April 5, 2001. Then Rule 11 adds the requirement to describe the substance of any consultations between the FBI and criminal prosecutors at DOJ or a United States Attorney's Office. The scope and degree of such consultations have proliferated significantly since promulgation of the AG's memo on information sharing on March 6, 2002, and access by prosecutors to intelligence information and to case files on intelligence investigations has reached unprecedented proportions

b5-1 b2-2 b7E-1



b5-1
b2-2 b7E-1

73



Certification

Subsection 104(a)(7) of FISA requires a certification by the Assistant to the President for National Security Affairs -- or other Executive Branch official designated by the President from among those officials employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate. The designated presidential advisor is the only one specifically provided for in the statute. By Executive Orders 12139 and 12949 the President has also designated the Director (and Deputy) of Central Intelligence, the Secretary (and Deputy) of Defense, the Secretary (and Deputy) of State and the Director of the FBI. Note that the Deputy Director of the FBI is conspicuously absent -- the Deputy Director is typically a career Special Agent rather than an official appointed by the President with the advice and consent of the Senate and therefore does not meet the statutory prerequisites.

Foreign Intelligence Information

The certification consists of five elements, the first of which is that the official making the certification deems the information sought to be foreign intelligence information. If you relate these officials and their functions to the definition of "foreign intelligence information" in section 101(e) of the statute, there is a certain attraction of logic in their selection. Under subsection 101(e)(1), "foreign intelligence information" means information that relates to [or, 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. These elements go to the classic counterintelligence and counterterrorism functions of the CIA and the FBI.

Under subsection 101(e)(2), the definition of "foreign intelligence information" includes information with respect to a foreign power or foreign territory that relates to [or, if concerning a United States person, is *necessary* to] (a) the national defense or the security or (B) the conduct of the foreign affairs of the United States. These elements implicate the missions and functions of the Secretary of Defense and the Secretary of State.

Under the scheme set up by Executive Order 12333, the Assistant to the President for National Security Affairs (the "National Security Advisor") is the senior Executive Branch official in the Intelligence Community and has interests in *all* of these matters.

The requirement that the certifier deems the information sought to be "foreign intelligence information" is designed to ensure that a senior official with responsibilities in the area of national security reviews the determination made at lower levels of the Executive Branch that the information sought is foreign intelligence information. The intent of FISA is ensure that the certifier carefully considers the substance of cases before him and does not simply sign off on boilerplate language. This prevents targeting a foreign power for electronic surveillance when the true purpose is to gather information about an individual for other than foreign intelligence purposes. It is also designed to make explicit that a significant purpose of such surveillance is to obtain "foreign intelligence information" as defined, rather than some other type of information. The certifier similarly must explain in his affidavit why the information cannot be obtained through less intrusive techniques. This requirement is particularly important when U.S. persons are the targets of surveillance or search.

A Significant Purpose

b5-1
b2-2 b7E-1

74

The second element of the certification is that "a significant purpose" of the surveillance or search is to obtain foreign intelligence information. Since the objective in enacting the statute is to provide a statutory procedure for the government to obtain a judicial order for electronic surveillance or physical search for foreign intelligence purposes, the "purpose" aspect of the certification is extremely important. The majority of pre-FISA caselaw had recognized a "national security exception" to the warrant requirement of the Fourth Amendment. In determining whether the cases before them should be accorded that exception, the courts tended to focus on whether the collection of foreign intelligence information was the "primary" purpose of the surveillance. In the case of *Humphrey and Truong* the trial judge concluded that the fruits of electronic surveillance and physical searches conducted without a warrant were admissible under the Fourth Amendment, provided those surveillances and searches had been conducted for a foreign intelligence purpose. The measure by which he determined purpose was direction and control of the surveillance, or investigation. So long as special agents of the FBI who normally investigated intelligence activities were directing and controlling the investigation, he construed the information as having been obtained for a foreign intelligence purpose. Conversely, when DOJ prosecutors began to write prosecutive memoranda and to control the direction of the investigation, he concluded that the information had been obtained for the purpose of prosecution and, accordingly, was inadmissible since it had been obtained without a warrant.

When FISA was enacted, it required that "the purpose" of the surveillance be to obtain foreign intelligence information. Based on experience with pre-FISA caselaw, the government's practice before the Foreign Intelligence Surveillance Court has been to construe "the purpose" as "primary purpose" and to determine purpose by following a procedure similar to that adopted in *Humphrey and Truong*. A reading of the legislative history of FISA suggests that subsection 104(a)(7) was intended to replace the *Humphrey-Truong* test with the accountable official's certification that the purpose of the surveillance or search is to acquire foreign intelligence information, as defined. The USA PATRIOT Act amended FISA to require that obtaining foreign intelligence information be a "significant" purpose of the surveillance or search. While there is a dearth of legislative history of this amendment, it would appear that the Congress intended to rectify perceived lapses in the government's handling of certain counterintelligence investigations with regard to the determination of probable cause to believe that he was an agent of a foreign power and to steer the government -- as well as the Foreign Intelligence Surveillance Court -- toward the statutory scheme of relying on the certification for determining purpose.

The information required by the FISC's Rule 11 is largely a recitation of criminal justice pursuits and appears to follow the pre-enactment practice of determining purpose through an examination of direction and control of the investigation. The Court's position in this regard was reiterated in its opinions of April 22 and May 17, 2002, regarding the AG's March 6, 2002, memo on information sharing. The certification required by subsection 104(a)(7) is not so much an analysis of direction and control as an affirmation of the intelligence objectives of the surveillance or search. The point for field agents to understand is that in submitting a request for initiation of FISA surveillance or search, it is important to articulate the specific intelligence objectives of the requested FISA coverage. *E.g.*, in an espionage case, those objectives might include identification of a subject's handler, or his tradecraft in servicing dead-drops or how he obtains access to classified information. In the case of a terrorism subject, the objectives of the surveillance might be to learn the extent of the subject's relationship with an international terrorist group. To ensure that the Director has a proper basis for making this certification, NSLU recommends that any communication to HQ requesting application to the Court for authorization to use a FISA technique should both articulate the intelligence objectives to be achieved through the use of FISA techniques and, to satisfy requirements imposed by the Court, describe any criminal aspect of the investigation in sufficient detail to determine that intelligence officials and not law enforcement officials are directing and controlling the use of FISA techniques.

Not Reasonably Obtainable by Other Means

The third element of the certification is that the information sought cannot reasonably be obtained by normal investigative techniques. There is not much legislative guidance on this requirement, but, in general terms, it appears to is based on the general principle -- subsequently reiterated in Executive Order 12333 -- that the Intelligence Community should respect individual privacy rights by conducting intelligence activities using the least intrusive techniques feasible. Thus, it would appear that, due to their intrusiveness, Congress intended FISA techniques should be a last -- rather than first -- resort. In most instances, this requirement can be satisfied by the fact that only surveillance or search of the kind authorized pursuant to FISA can adequately obtain the information sought. For example, if more visible or detectable means of surveillance were utilized, the subject would likely change his means of communication to something less susceptible of surveillance.

Category of Foreign Intelligence Information Sought

The fourth aspect of the certification is designation of the type of foreign intelligence information being sought according to the categories described in section 101(e) of the statute, whether one of the kinds of counterintelligence information defined in subsection 101(e)(1), or of positive intelligence as defined in subsection 101(e)(2).

Basis for Certification

The final part of the certification is a statement of the basis for the certification as to the third and fourth elements, *i.e.*, that the information sought is the type of foreign intelligence information designated, and that such information cannot reasonably be obtained by normal investigative techniques. Usually this is based on the results of the FBI's investigation to date. A presentation of facts relevant to this issue might follow a logical flow of relating the activities of the target that make him an "agent of a foreign power" as defined in subsection 101(b) to the appropriate definition of "foreign intelligence information" in subsection 101(e), coupled with a discussion of the technique that would be necessary to obtain that kind of intelligence information. This element of the certification is not required when the target of the electronic surveillance is a foreign power as defined in subsection 801(a)(1), (2) or (3), *i.e.*, a foreign government or component thereof; a faction of a foreign nation not substantially composed of United States persons; or an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments.

Duration

The general rule is that the FISC may approve electronic surveillance for the period necessary to achieve its purpose, or for 90 days, whichever is less. There are certain exceptions. Electronic surveillance of a foreign power as defined in section 101(a)(1), (2) or (3) may be authorized for up to one year. Electronic surveillance of a foreign agent as defined in section 101(b)(1)(A) may be for the period specified in the application or for 120 days, whichever is less. Upon renewal, surveillance of a 101(b)(1)(A) agent of a foreign power may be for a period not to exceed one year.

An order authorizing physical search may be approved for the period necessary to achieve its purpose, or for 90 days, whichever is less. As with electronic surveillance, there are exceptions. Physical search of a foreign power, as defined in 101(a)(1), (2) or (3), may be authorized for the period specified in the application or for one year, whichever is less, and physical search of a section 101(b)(1)(A) agent of a foreign power may be authorized for the period specified in the application or for 120 days, whichever is less. An extension may be granted for a period not to exceed one year if the judge finds probable cause to believe that no property of any individual United States person will be acquired during the period in which search is authorized.

It is important to ensure that surveillance or searches adhere to the timelines specified in the orders. For one thing, the length of time involved in drafting a FISA application and preparing it for presentation to the Court requires that requests for renewal be forwarded in timely fashion. You cannot wait until two weeks before an order expires to submit a request for the next one. It is also imperative that actual surveillance or search not occur beyond the period of authorization specified in the order. If surveillance should overrun the period of authorization, any unauthorized "take" must be sequestered and forwarded to the Office of Intelligence Policy and Review, via the substantive unit at FBIHQ, for submission to the Foreign Intelligence Surveillance Court. The overrun must also be reported by electronic communication to the Inspection Management Unit of the Inspection Division within 14 days of discovery of the error. [See section 2-56.E of the National Foreign Intelligence Program Manual.]

Miscellaneous Considerations

Getting an order from the Court is only the beginning of the successful administration of the authorities granted pursuant to FISA. Among the practical considerations that should attend implementation of a FISA order is ensuring that the "premises" being surveilled are those named in the order. For example, it is important to ensure that telephone coverage is on the right telephone line. Clues that something is amiss might include the fact that intercepted communications are in a language other than that expected. Or the information obtained might appear to be non-pertinent to the intelligence objectives of the surveillance.

76

In cases of physical search, the Court typically requires a re[illegible]by the federal officer executing the search. The return is essentially a report to the Court of the circumstances under which the search was conducted and the information or tangible items seized. It is common for the Court to require a return within twenty-one (21) days of the execution of a search, but 21 days is not necessarily applicable to all cases, so it is important to note the specific requirements of individual orders.

Another practical consideration is the provision of subsection 105(c)(2) that the Court may order a communications common carrier, landlord, custodian or other specified person to furnish the applicant [the FBI] with all information, facilities or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy. In addition, the Court may order such persons maintain any records concerning the surveillance or the aid furnished that such person wishes to retain under security procedures approved by the Attorney General and the Director of Central Intelligence. Subsection 304(c)(2) makes similar provision for physical searches.

A recurring problem is service of the order on service providers or other specified persons who lack security clearances or, in some cases, the wherewithal to store classified orders properly. When FISA was originally enacted, the overwhelming bulk of the surveillance was simple telephone wiretaps, and there were only a few large communications common carriers with which to deal. As a result, it was relatively easy to obtain clearances for a security office at a large carrier to obtain proper access to information and storage facilities. Since then, however, the large telephone companies have broken up into numerous "baby bells," leading to a proliferation of the workload involved with background investigations and clearances. In addition, the advent of the Internet and the concomitant proliferation of Internet service providers have also added to investigative and security clearance workloads.

The security procedures approved by the Attorney General and the Director of Central Intelligence empower the SAC to authorize disclosure of a classified order on an emergency basis under circumstances in which such disclosure is necessary to execute the order. As a rule, the classified information contained in a secondary order is typically limited to identification of the target -- which information is frequently communicated to the service provider anyway in preliminary discussion. As a result, showing a service provider the secondary order typically amounts to disclosure of something he already knows -- the identity of the subject of surveillance. In a case in which an ongoing relationship is not likely and there is no need for the service provider to have longterm access to classified information, the SAC may authorize showing the secondary order to a service provider or other specified person on a one-time basis. It is recommended that the service provider be offered a "trust receipt" that relates back to the order by date and docket number and that the field office secure the secondary order. The service provider should be advised that the order will be made available should the need arise. If needed, a copy of the security procedures [which are classified] and a model trust receipt may be obtained from NSLU via Groupwise e-mail.

With regard to the trust receipt, the most common concern expressed by service providers is the fear of being sued for providing assistance to the FBI. Service providers may be advised of the following provision of subsection 105(i):

> No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act for electronic surveillance or physical search.

In addition to this statutory protection from civil liability, if a service provider were to be sued for assisting the FBI in conducting electronic surveillance or physical search pursuant to FISA, the Bureau would seek the Attorney General's assertion of the State Secrets Privilege [*United States v. Reynolds*, 345 U.S. 1 (1953)] to prevent the disclosure of classified information that would be required to sustain such a cause of action. If a field office is contacted by a service provider about such a situation, NSLU should be notified immediately.

Coming Attractions . . .

The gathering of information, including information as to the capabilities, intentions and activities of foreign powers and their agents, would be meaningless without successful exploitation of that information to protect the

77

United States from hostile attack and other grave acts, acts of terrorism, sabotage and clandestine intelligence activities. Bearing in mind that the recurring theme in various provisions of FISA is the balancing of individual rights to privacy against the need of the government's need to acquire and produce foreign intelligence information, FISA creates a heavy burden with regard to managing the acquisition, retention and dissemination of U.S. person information. In sum, this is the process of "minimization." As most minimization procedures are classified, minimization is not addressed here in detail. In addition, the procedures for "information sharing" promulgated by the Attorney General on March 6 and modified somewhat by the FISA Court are still subject to judicial review. Accordingly, procedures for the sharing of information will be the subject of a separate communication.

Top of Page

Last Updated: Thursday, September 12, 2002

78