CHAPTER TWO
BACKGROUND

I. Introduction

This chapter provides a description of key terminology, the FBI's organizational structure, and legal background related to an examination of how the FBI investigated international terrorism matters before the September 11 terrorist attacks.[5] It also provides a basic overview of the legal issues and policies that affected how the FBI typically handled terrorism investigations before September 11, 2001.[6]

A. Introduction to international terrorism

The FBI defines terrorism as the unlawful use or threatened use of violence committed against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. When such violent acts are carried out by a group or individual based and operating entirely within the United States without foreign direction, they are considered acts of domestic terrorism, such as the April 1995 bombing of the Alfred P. Murrah federal building in Oklahoma City, Oklahoma. When such acts are committed by an individual or group based or operating outside of the United States, they are considered acts of international terrorism, such as the September 11, 2001, attacks on the World Trade Center and the Pentagon. See the FBI's National Foreign Intelligence Program Manual, Section 2-1.1.

According to the FBI, there are three main categories of international terrorist threats to U.S. interests: formal, structured terrorist organizations;[7]

---

[5] A list of acronyms used in this report is attached in the Appendix.

[6] Those who have such knowledge may not need to read this chapter and can go directly to the chapters of the report detailing our investigation of the FBI's handling of specific matters, beginning with Chapter Three's discussion of the Phoenix EC.

[7] Formal, structured terrorist organizations are those with their own personnel, infrastructures, financial arrangements, and training facilities. Such groups include al Qaeda, the Palestinian Hamas, the Irish Republican Army, the Egyptian Al-Gama Al- (continued)

state sponsors of international terrorism[8]; and loosely affiliated Islamic extremists.[9] According to Dale Watson, the former Executive Assistant Director for Counterterrorism, the trend in international terrorism has been a shift away from state sponsors of terrorism and formalized terrorist organizations towards loosely affiliated religious extremists who claim Islam as their faith.

Among these Islamic extremists is Usama Bin Laden, who heads the al Qaeda transnational terrorist network. Al Qaeda leaders were harbored in Afghanistan by the Taliban regime from 1996 until the U.S. military operations there in 2001. In addition to the September 11 attacks, al Qaeda was responsible for the bombing of the *U.S.S. Cole* in Yemen on October 12, 2000, the bombings of the U.S. Embassies in Kenya and Tanzania in August 1998, and numerous other terrorist attacks.

B. The FBI's role in protecting against international terrorism

A critical part of the effort to prevent terrorism is the collection of timely and accurate intelligence information about the activities, capabilities, plans and intentions of terrorist organizations. The U.S. "Intelligence Community" is composed of 14 U.S. agencies responsible for collecting intelligence information on behalf of the government.[10]

(continued)
Islamiyya, and the Lebanese Hizbollah. Hizbollah, for example, carried out numerous attacks on Americans overseas, including the October 1983 vehicle bombing of the U.S. Marine barracks in Lebanon and the June 1996 bombing of Khobar Towers in Saudi Arabia.

[8] According to the FBI, as of 2001 the primary state sponsors of terrorism were Iran, Iraq, Sudan, and Libya.

[9] This is sometimes referred to as the "Islamic Jihad Movement" or the "International Jihad Movement."

[10] These 14 agencies are: the CIA, FBI, Defense Intelligence Agency (DIA), National Security Agency (NSA), U.S. Army Intelligence, U.S. Navy Intelligence, U.S. Air Force Intelligence, U.S. Marine Corps Intelligence, National Geospatial Agency (NGA), National Reconnaissance Office (NRO), Department of the Treasury, Department of Energy, Department of State, and the Coast Guard. The Director of Central Intelligence (the DCI) oversees the Intelligence Community and also serves as the principal advisor to the President for intelligence matters and as the Director of the CIA.

The National Security Act of 1947 created the Central Intelligence Agency (CIA) and established it as the United States' lead intelligence agency. The CIA engages primarily in the collection of foreign intelligence information, which is information relating to the capabilities, intentions, and activities of foreign governments or organizations, including information about their international terrorist activities. The Act prohibits the CIA from exercising any "police, subpoena, law enforcement powers, or internal security functions."

The FBI is the nation's lead agency for the collection of "foreign counterintelligence information."[11] According to the Attorney General Guidelines in place at the time, which were called the Attorney General Guidelines for Foreign Counterintelligence (FCI) Investigations, FCI is information relating to espionage and other intelligence activities, sabotage, or assassinations conducted by, for, or on behalf of foreign governments or organizations, as well as information relating to international terrorist activities. Intelligence investigations include investigations of individuals who are international terrorists, groups or organizations that are engaged in espionage; or groups or organizations that are engaged in international terrorism.

The FBI can initiate an intelligence investigation even if a crime has not been committed. For example, the FBI may investigate and collect intelligence information about an individual who is believed to be an international terrorist or a spy without showing that the individual has participated in any terrorist act or actually committed espionage. Intelligence investigations are distinguishable from criminal investigations, such as bank robbery or drug trafficking investigations, which attempt to determine who committed a crime and to have those individuals criminally prosecuted. Prevention of future terrorist acts rather than prosecution after the fact is the primary goal of the intelligence investigations with respect to international terrorism matters.

---

[11] The authority for the FBI's broad mission to act as the nation's lead domestic intelligence agency is set forth most clearly in Presidential Executive Order 12333, implemented on December 4, 1981.

International terrorism could be investigated as both an intelligence investigation and as a criminal investigation. When a criminal act, such as the bombing of a building, was determined to be an act of international terrorism, the FBI could open a criminal investigation and investigate the crime, as it did other criminal cases, with the goal of prosecuting the terrorist.[12] At the same time, the FBI could open an intelligence investigation of an individual or a group to investigate the person's contacts, the group's other members, the intentions of the individual or the group, or whether any future terrorist act was planned.[13]

One significant difference between an intelligence investigation and a criminal investigation is the legal framework that applies when a physical search or electronic surveillance is initiated.[14] In a criminal investigation that implicates the privacy interests protected by the Fourth Amendment, the general rule is that searches may not be conducted without a warrant issued by a magistrate upon a finding that probable cause exists that evidence of a crime will be uncovered.[15] When the FBI seeks to conduct electronic surveillance in a criminal investigation, the FBI must obtain a warrant by complying with the requirements of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2522 (Title III). When a physical search is sought in

---

[12] The FBI has been assigned "lead agency responsibilities" by the Attorney General to investigate "all crimes for which it has primary or concurrent jurisdiction and which involve terrorist activities or acts in preparation of terrorist activities within the statutory jurisdiction of the United States." National Security Directive 207, issued in 1986, specifically assigned responsibility to the FBI for response to terrorist attacks, stating: "The Lead Agency will normally be designated as follows: The Department of Justice for terrorist incidents that take place within U.S. territory. Unless otherwise specified by the Attorney General, the FBI will be the Lead Agency within the Department of Justice for operational response to such incidents."

[13] After the attacks of September 11, 2001, the FBI significantly changed how it investigates international terrorism cases. We discuss those changes throughout this report.

[14] Electronic surveillance includes wiretapping of telephones, installing microphones in a house or building, and intercepting computer usage. Electronic surveillance is considered a particular kind of search.

[15] There are several exceptions to the warrant requirement that are not material to this report.

a criminal investigation, the FBI also must comply with the requirements of Rule 41 of the Federal Rules of Criminal Procedure.

With respect to an intelligence investigation, however, criminal search warrants issued by a magistrate are not required. The courts have long recognized the Executive Branch's claim of inherent constitutional power to conduct warrantless surveillance to protect national security.[16] However, because such authority was abused, Congress created procedures and judicial oversight of the Executive Branch's exercise of this authority with the passage of the Foreign Intelligence Surveillance Act of 1978 (FISA).[17] 50 U.S.C. §1801 *et seq*. FISA requires the FBI to obtain an order from the Foreign Intelligence Surveillance Court (FISA Court) upon a showing of probable cause to believe that the subject of the surveillance is a foreign government or organization engaging in clandestine intelligence activities or international terrorism, or is an individual engaging in clandestine intelligence activities or international terrorism on behalf of a foreign government or organization.[18] In addition, prior to September 11, 2001, the government had to submit a certification to the FISA Court that "the purpose" of the surveillance or search was collection of "foreign intelligence information."[19] 50 U.S.C. § 1804(a)(7)(E).

---

[16] The U.S. Constitution, Article II, Section 1, clause 7, supplies the President's constitutional mandate to "preserve, protect and defend the Constitution of the United States."

[17] Among the most notable examples of the Executive Branch's abuse of this authority was action taken in relation to the Watergate scandal.

[18] Prior to September 11, 2001, the FISA Court consisted of seven federal district court judges designated by the Chief Justice of the Supreme Court, at least one of whom was a member of the federal district court in Washington, D.C. After September 11, 2001, the number of FISA Court judges was increased to 11. The government presents applications for a court order authorizing electronic surveillance or a physical search to the judges in *in camera, ex parte* proceedings. FISA also created the Foreign Intelligence Surveillance Court of Review, which has jurisdiction to review the denial of FISA applications by the FISA Court.

[19] The FISA statute provides that the FBI must show that "the target of the electronic surveillance is a foreign power or an agent of a foreign power." 50 U.S.C. § 1804(a). These terms and requirements are discussed in more detail in Section IV, A below.

II. The FBI's organizational structure with respect to international terrorism

The FBI's Counterterrorism Program is responsible for supervising and handling FBI terrorism matters. Before September 11, 2001, the Counterterrorism Program was housed in the Counterterrorism Division at FBI Headquarters.[20] International terrorism and domestic terrorism were subprograms within the Counterterrorism Program.

A. Counterterrorism Program

Although the FBI has had primary responsibility since 1986 for investigating and preventing acts of terrorism committed in the United States, the FBI developed its formal Counterterrorism Program in the 1990s. For much of the 1990s, terrorism matters were overseen at FBI Headquarters by about 50 employees in the counterterrorism section within the FBI's National Security Division (later called the Counterintelligence Division). The National Security Division also managed the FBI's Foreign Counterintelligence Program. According to Dale Watson, former Executive Assistant Director for Counterterrorism, in the early 1990s counterterrorism was considered a "low-priority program" in the FBI.

According to Watson's testimony before the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence on September 26, 2002, the first attack on the World Trade Center in February 1993 and the April 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma, were "confirmation" that terrorist acts could be committed on U.S. soil. Watson testified that the World Trade Center bombing in 1993 was a "wake-up call" and that prior to this attack and the Oklahoma City bombing "terrorism was perceived as an overseas problem."

In addition to the FBI's counterterrorism efforts, the CIA has for years focused on international terrorism in general and Usama Bin Laden in particular. In 1986, the CIA established a Counterterrorist Center (CTC) at

---

[20] The FBI has reorganized its Counterterrorism Program several times since September 11, 2001. We provide in this section of the report the description of the organization and positions that existed immediately prior to the September 11 attacks.

CIA Headquarters after a task force concluded that U.S. government agencies had not aggressively operated to disrupt terrorist activities. The CTC's stated mission is to preempt, disrupt, and defeat terrorists by implementing a comprehensive counterterrorist operations program to collect intelligence on and minimize the capabilities of international terrorist groups and state sponsors of terrorism. The CTC attempts to exploit source intelligence to produce in-depth analyses on potential terrorist threats and coordinate the Intelligence Community's counterterrorist activities.

CIA Director George Tenet testified before Congress that Usama Bin Laden came to the attention of the CIA as "an emerging terrorist threat" during his stay in Sudan from 1991 to 1996. As early as 1993, the CIA began to propose action to reduce his organization's capabilities. Tenet stated that the Intelligence Community was taking action to stop Bin Laden by 1996, when he left Sudan and moved to Afghanistan.

In 1996, the CIA established a special unit, which we call the Bin Laden Unit, to obtain more actionable intelligence on Bin Laden and his organization.[21] This effort was the beginning of an exchange program between the FBI and the CIA in which senior personnel moved temporarily between the two agencies.

Around the same time, in April 1996 the FBI created its own Counterterrorism Center at FBI Headquarters. As part of the Counterterrorism Center, the FBI established an exchange of working-level personnel and managers with several government agencies, including the CIA, Immigration and Naturalization Service (INS), the Federal Aviation Administration (FAA), and others.

In May 1998, a task force of FBI officials created a 5-year strategic plan for the FBI, based on a 3-tier system, setting investigative priorities that would affect the allocation of FBI resources. Tier 1 included crimes or intelligence problems that threatened national or economic security. Counterterrorism was

---

[21] The Bin Laden Unit was housed organizationally within the CTC during the time period most relevant to this report. Around September 11, 2001, approximately 40-50 employees worked in the Bin Laden Unit. We discuss the Bin Laden Unit in more detail in Chapter Five.

designated a Tier 1 priority. Tier 2 involved criminal enterprises or those offenses that adversely affected public integrity, and Tier 3 included crimes that affected individuals or property.

In November 1999, the FBI took the Counterterrorism Program out of the National Security Division and created a separate Counterterrorism Division.

1. Organization of the Counterterrorism Division

The major components of the FBI's Counterterrorism Division prior to September 11, 2001, were the International Terrorism Operations Section (ITOS), the Domestic Terrorism Operations Section (DTOS), the National Infrastructure Protection Center (NIPC), and the National Domestic Preparedness Office (NDPO).[22]

The issues in this report focus primarily on ITOS, which was responsible for overseeing the FBI's international terrorism investigations, both criminal and intelligence investigations. The mission of the ITOS was twofold: to prevent terrorist acts before they occurred, and if they occurred to mount an effective investigative response with the goal of prosecuting those responsible.

Prior to September 11, 2001, approximately 90 employees worked in ITOS at FBI Headquarters. ITOS was led by Section Chief Michael Rolince during the time relevant to this report.

ITOS was divided into several units. One of those units handled Bin Laden-related investigations, and was called the Usama Bin Laden Unit or the UBLU. Cases that could not be linked to a specific group and that involved radical

---

[22] The NIPC, created in February 1998, was originally called the Computer Investigation and Infrastructure Threat Center. The NIPC's mission was to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against the nation's critical infrastructures. These infrastructures include telecommunications, energy, banking and finance, water systems, government operations, and emergency services. The NDPO was created in October 1998 to coordinate all federal efforts to assist state and local law enforcement agencies with the planning, training, and equipment needs necessary to respond to a conventional or non-conventional weapons of mass destruction incident. The NIPC has since been moved to the Department of Homeland Security. The responsibilities for the NDPO were moved to the Federal Emergency Management Agency before September 11, 2001.

extremist allegations were assigned to Radical Fundamentalist Unit or the RFU. Before September 11, it had approximately ten employees.

2. Management of counterterrorism cases at FBI Headquarters

FBI Headquarters was more closely involved in overseeing counterterrorism investigations compared to criminal cases such as bank robberies or white collar crime. In counterterrorism cases, FBI Headquarters was responsible for, among other things, ensuring that intelligence information received from outside agencies was provided to the relevant field offices and assisting field offices in preparing the paperwork necessary to apply for a FISA order. For this reason, we discuss the duties of the relevant personnel at FBI Headquarters with respect to counterterrorism investigations.

a. Supervisory Special Agents and Intelligence Operations Specialists

Each of the five units within ITOS was staffed by several Supervisory Special Agents (SSA), each of whom worked closely with Intelligence Operations Specialists (IOS). The SSAs were FBI agents who had several years of experience in the field and had been promoted to a supervisory headquarters position. These SSAs generally worked in ITOS for approximately two years before becoming supervisors in a field office or elsewhere in FBI Headquarters. ITOS SSAs typically had at least some experience in terrorism matters prior to coming to ITOS.

IOSs were non-agent, professional employees.[23] Some had advanced degrees in terrorism or terrorism-related fields. Others had no formal training in analytical work but advanced to their IOS positions from clerical positions within the FBI. Most IOSs were long-term employees who were expected to have institutional knowledge about terrorism matters, such as the history of a particular terrorist organization or the principal participants in a terrorist organization.

---

[23] In October 2003, the FBI reclassified all FBI analysts under one position title – Intelligence Analyst. IOSs now are called "Operations Specialists."

The responsibilities of each SSA and IOS depended on the unit in which they worked. Some SSAs and IOSs oversaw all FBI investigations relating to a particular terrorist group or a particular target. Other SSAs and IOSs were responsible for overseeing terrorism investigations conducted in a particular region of the country.

SSAs and IOSs were the first point of contact for agents and supervisors in the field conducting counterterrorism investigations when approval, advice, or information was needed. For example, if a field office's investigation revealed connections between the subject of the investigation and a known leader of a terrorist organization, the IOS was supposed to provide the field office with the FBI's information on the leader of the terrorist organization. In addition, SSAs and IOSs assisted field offices by assembling the necessary documentation to obtain court orders authorizing electronic surveillance pursuant to FISA. This is discussed further in Section IV, B below.

SSAs and IOSs also were responsible for collecting and disseminating intelligence and threat information. They received information from various FBI field offices and from other intelligence agencies that needed to be analyzed and disseminated to the field. SSAs and IOSs also acted as liaisons with other intelligence agencies. They also received information from these agencies in response to name check requests or traces on telephone numbers as well as intelligence and threat information.

With respect to threat information, SSAs and IOSs worked with FBI field offices or Legal Attaché (Legat) offices to assess the threat and take any action necessary to prevent terrorist acts from occurring.[24] For example, an IOS would conduct research on the names associated with the threats, arrange for translators to translate any intercepts from electronic surveillance, request information from other agencies about the persons associated with the threats, and prepare communications to the field office and Legat to ensure that

---

[24] Prior to September 11, 2001, the FBI had 44 Legat offices around the world. Legat offices assist the FBI in its mission from outside of the United States by, for example, coordinating with other government agencies to facilitate the extradition of terrorists wanted for killing Americans. As of June 2004, the FBI had 45 Legat offices and four Legat sub-offices.

updated information was provided to the necessary persons involved in the investigation.

b. Intelligence Research Specialists and analysis within the Counterterrorism Division

Prior to September 11, 2001, Intelligence Research Specialists (IRSs) also were a part of the FBI's Counterterrorism Program, although they were housed in a separate division of the FBI from the SSAs and IOSs. Both IRSs and IOSs performed an important function in the intelligence arena called "analysis."

Analysis is the method by which pieces of intelligence information are evaluated, integrated, and organized to indicate pattern and meaning. As information is received, it must be examined in-depth and connected to other pieces of information to be most useful.

Analysis generally is considered to be either tactical or strategic. Tactical analysis, which also is called operational analysis, directly supports investigations or attempts to resolve specific threats. It normally must be acted upon quickly to make a difference with respect to an investigation or a threat. An example of tactical analysis is the review of the telephone records of several subjects to determine who might be connected to whom in a certain investigation or across several investigations. Another example of tactical analysis is a review of case files to determine whether similar, suspicious circumstances in two unrelated police reports exist in other cases and are somehow connected to each other or to criminal or terrorist activity.

In contrast to tactical analysis, strategic analysis provides a broader view of patterns of activity, either within or across terrorism programs. Strategic analysis involves drawing conclusions from the available intelligence information and making predictions about terrorist activity. It is not simply descriptive but proactive in nature. A typical product of strategic analysis is a report that includes program history, shifts in terrorist activity, and conclusions about how the FBI should respond.

The FBI has acknowledged that prior to September 11, 2001, its Counterterrorism Division was primarily geared toward conducting tactical

analysis in support of operational matters rather than strategic analysis.[25] Tactical analysis generally was handled by IOSs within the operational units.

Prior to September 11, strategic analysis for the Counterterrorism Division was performed by IRSs. Like IOSs, IRSs were non-agent, professional employees who were expected to be subject matter experts about a particular terrorism group, program, or target. All IRSs at the FBI had college degrees, and some had advanced degrees. Like IOSs, IRSs were expected to be long-term FBI employees who possessed the "institutional knowledge" about a particular program or target.[26]

During the time period relevant to our review, IRSs who worked counterterrorism matters were assigned to the Investigative Services Division (ISD), a division separate from the Counterterrorism Division that contained all IRSs in the FBI. IRSs were grouped in units and reported to a unit chief, who reported to a section chief. The IRSs who were assigned to the FBI's Counterterrorism Program typically worked with the same SSAs and IOSs assigned to a particular terrorist group or target. For example, an IRS who was assigned to Bin Laden matters typically worked with IOSs and SSAs in the UBLU in ITOS.

As we discuss in detail in Chapter Three, the number of FBI IRSs decreased significantly before September 11, 2001, and the relatively few IRSs were often used to perform functions other than strategic analysis.

Many FBI analysts and supervisors noted to the OIG that the resources devoted to the Counterterrorism Program and analysis were inadequate, and that the amount of work in the Counterterrorism Program was overwhelming. They also stated that they were hampered significantly by inadequate technology. We discuss these issues in further detail in Chapter Three of the report on the handling of the Phoenix EC. However, these difficult conditions in the Counterterrorism Program apply equally to the issues in the other chapters in our report.

---

[25] In Chapter Three, we discuss in more detail the FBI's lack of strategic analysis capabilities prior to September 11, 2001.

[26] IRSs now are called "All Source Analysts."

B. Field offices and counterterrorism investigations

Prior to September 11, 2001, FBI counterterrorism investigations, whether intelligence or criminal, were opened and led by the FBI's 56 field offices. In many field offices, counterterrorism investigations were handled by a squad that focused on terrorism cases only. In the New York Field Office and other large offices, several squads were devoted solely to international terrorism matters. In smaller field offices, international terrorism and domestic terrorism investigations often were assigned to the same squad. FBI agents generally developed specialties within the terrorism field such as a particular terrorist organization. Each squad was led by an SSA who reported to an Assistant Special Agent in Charge (ASAC) who, in turn, reported to the Special Agent in Charge (SAC).[27]

As stated above, field offices opened international terrorism investigations as either a criminal investigation or an intelligence investigation. Attorney General Guidelines delineated the information or allegations that were necessary to open a criminal investigation or an intelligence investigation.[28]

For both criminal and intelligence cases, the Attorney General Guidelines set forth the criteria for opening two levels of investigations – a "preliminary inquiry" (PI) and a "full investigation" (also called a full field investigation or FFI). The Guidelines also specified what investigative techniques could be employed in preliminary inquiries or full investigations. Both sets of the

---

[27] In larger field offices such as New York, several SACs report to an Assistant Director in Charge (ADIC).

[28] Separate Attorney General Guidelines regulate the FBI's conduct in criminal investigations, intelligence investigations, and the handling of informants, among other issues. The Attorney General Guidelines that addressed criminal investigations were called "The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations" (hereinafter "criminal AG Guidelines"). The Attorney General Guidelines in effect at the time that addressed intelligence investigations were labeled "Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations" (hereinafter "FCI AG Guidelines"). Revised criminal Attorney General Guidelines were issued on May 30, 2002, and new FCI Guidelines were issued on October 31, 2003.

Guidelines provided that preliminary inquiries were conducted to determine whether a basis existed for a full investigation. However, preliminary inquiries had to be closed when there was insufficient information after a certain period of time to support opening a full field investigation.

With respect to intelligence cases, agents could collect information by, among other methods, questioning sources, finding new sources, checking FBI and other agency databases, and reviewing intelligence information from other intelligence agencies. Information was recorded in the form of Electronic Communications (ECs) that became part of the case file. An EC is the standard form of communication within the FBI.

Before September 11, 2001, FBI international terrorism intelligence cases contained the case identifier number 199. Letter or "alpha" designations were also used, along with the case identifier, to further identify intelligence investigations. For example, intelligence investigations related to a particular terrorist organization were designated as 199N investigations. International terrorism intelligence investigations often are referred to as "a 199." A criminal international terrorism investigation had the FBI case identifier number 265; these investigations were commonly referred to as "a 265."[29]

C. The Department's Office of Intelligence Policy and Review

As mentioned above, when the FBI conducts intelligence investigations, a significant tool for uncovering information is the FISA statute. The FBI obtains an order from the FISA Court authorizing electronic surveillance and searches with the assistance of Department attorneys in the Office of Intelligence Policy and Review (OIPR). OIPR is under the direction of the Counsel for Intelligence Policy.[30]

---

[29] Currently, the FBI uses only one designation for international terrorism investigations.

[30] We discuss in detail the process for obtaining FISA warrants and the role of FBI and OIPR personnel in this process in Section IV, B.

III. The wall between intelligence and criminal terrorism investigations

A. Introduction

This section summarizes the creation of the "wall" separating criminal and intelligence terrorism investigations in the Department of Justice. The wall began as a separation of intelligence investigators from contact with criminal prosecutors, and evolved to include a separation of FBI investigators working on intelligence investigations from investigators working on criminal investigations.

As discussed above, FBI terrorism investigations could be opened either as an intelligence investigation in which information was collected for the protection of national security, or as a criminal investigation to prevent a criminal act from occurring or to determine who was responsible for a completed criminal act. In the course of an intelligence investigation, information might be developed from searches or electronic surveillance obtained under FISA. That intelligence information also could be relevant to a potential or completed criminal act. However, concerns were raised that if intelligence investigators consulted with prosecutors about the intelligence information or provided the information to criminal investigators, this interaction could affect the prosecution by allowing defense counsel to argue that the government had misused the FISA statute and it also could affect the intelligence investigation's ability to obtain or continue FISA searches or surveillances. As a result, procedural restrictions – a wall – were created to separate intelligence and criminal investigations. Although information could be "passed over the wall" – i.e., shared with criminal investigators – this occurred only subject to defined procedures.

The wall separating intelligence and criminal investigations affected both the Moussaoui case and the Hazmi and Mihdhar case. As we discuss in detail in Chapter Four, in the Moussaoui case FBI Headquarters believed that the Minneapolis agents should not contact the local U.S. Attorney's Office to seek a criminal warrant to search Moussaoui's possessions because, under the standards prior to September 11, 2001, contact with the local prosecutor would undermine any later attempt to obtain a FISA warrant. And as we discuss in detail in Chapter Five, because of the wall – and beliefs about what the wall required – an FBI analyst did not share important intelligence information about Hazmi and Mihdhar with criminal investigators. In addition, also

because of the wall, in August 2001 when the New York FBI learned that Hazmi and Mihdhar were in the United States, criminal investigators were not allowed to participate in the search for them.

Because the wall between intelligence and criminal investigations affected these two cases, we provide in this section a description of how the wall was created and evolved in response to the 1978 FISA statute. We also describe the unwritten policy separating criminal and intelligence investigations in the 1980s and early 1990s, the 1995 Procedures that codified the wall, the FISA Court procedures in 2000 that required written certification that the Department had adhered to the wall between criminal and intelligence investigations, and the changes to the wall after the September 11 attacks.

1. The "primary purpose" standard

The FISA statute, enacted in 1978, authorizes the FISA Court to grant an application for an order approving electronic surveillance or a search warrant to obtain foreign intelligence information if there is probable cause to believe that the target of the surveillance or search warrant is a foreign power or an agent of a foreign power. 50 U.S.C. § 1805(a)(3). The statute requires that the government certify when seeking the warrant that "the purpose" of the FISA search or surveillance is to obtain "foreign intelligence information." The statute states that the certification must be made "by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate." 50 USC § 1804(a)(7). Within the Department, the certification is usually signed by the FBI Director.

While Congress anticipated that evidence of criminal conduct uncovered during FISA surveillance would be provided to criminal investigators, the circumstances under which such information could be furnished to criminal investigators were not provided for in the statute.[31] Defendants in criminal

---

[31] The legislative history states that "surveillance to collect positive foreign intelligence may result in the incidental acquisition of information about crimes; but this is not its objective." Further, it states, "Surveillance conducted under [FISA] need not stop once conclusive evidence of a crime is obtained, but instead may be extended longer where (continued)

cases can challenge the government's use of information collected under a FISA warrant by arguing that the government's purpose in obtaining the information pursuant to FISA was not for collection of foreign intelligence, but rather for use in a criminal prosecution. Such a purpose would violate the Fourth Amendment's prohibition against warrantless searches, and could result in evidence obtained under FISA being suppressed in the criminal case. Alternatively, the FISA Court could reject an application for a FISA warrant because of concerns that the government's purpose for seeking the FISA warrant was for use in a criminal case rather than collecting foreign intelligence.

As a result, in interpreting FISA courts applied "the primary purpose" test. This allowed the use of FISA information in a criminal case provided that the "primary purpose" of the FISA surveillance or search was to collect foreign intelligence information rather than to conduct a criminal investigation or prosecution. The seminal court decision applying this standard to information collected in intelligence cases was issued in 1980. See United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980). In this case, the Fourth Circuit Court of Appeals ruled the government did not have to obtain a criminal warrant when "the object of the search or the surveillance is a foreign power, its agents or collaborators," and "the surveillance is conducted 'primarily' for foreign intelligence purposes." Id. at 915. However, the court ruled that the government's primary purpose in conducting an intelligence investigation could be called into question when prosecutors had begun to assemble a prosecution and had led or taken on a central role in the investigation.

Although the Truong decision involved electronic surveillance conducted before FISA's enactment in 1978, courts used its reasoning and applied the primary purpose test in challenges in criminal cases to the use of information gathered from searches or electronic surveillance conducted pursuant to FISA. See, e.g., United States v. Johnson, 952 F.2d 565 (1st Cir. 1991), cert. denied, 113 S.Ct. 58 (1992) ("[a]lthough evidence obtained under FISA subsequently may be used in criminal prosecutions, the investigation of criminal activity

---

(continued)
protective measures other than the arrest and prosecution are more appropriate." S. 1566, 95th Congress, 2d Session, Report 95-701, March 14, 1978.

cannot be the primary purpose of the surveillance"); United States v. Pelton, 835 F.2d 1067 (4th Cir. 1987), cert. denied, 486 U.S. 1010 (1988).

In the 1980s, the Department also adopted the "primary purpose" standard contained in the Truong case.[32] It interpreted the FISA statute as requiring prosecutors not to have control in intelligence investigations in which information was being collected pursuant to FISA. The concern was that too much involvement by prosecutors in the investigation created the risk that a court would rule that the FISA information could not be used in a criminal case because the "primary purpose" of the search was not the gathering of foreign intelligence.

As a result, during the 1980s and through the mid-1990s, the Department's policy was that prosecutors within the Department's Criminal Division – not attorneys in the local United States Attorneys' Offices (USAOs) – had to be consulted in connection with intelligence investigations in which federal criminal activity was uncovered, or when legal advice was needed to avoid investigative steps that might inadvertently jeopardize the option of prosecution using information obtained from the intelligence investigation. Criminal Division attorneys were briefed by the FBI about ongoing intelligence investigations and were expected to provide advice geared toward preserving a potential criminal case, but they were not allowed to exercise control over the investigation. The Criminal Division and FBI Headquarters made the policy decision about when to involve the USAO in the investigation, since consulting with the USAO was viewed as a bright line signifying the transition from an intelligence investigation to a criminal investigation. However, during this time period, no formal written guidelines governed the contacts between the FBI and the Criminal Division.

---

[32] The Foreign Intelligence Surveillance Court of Review later noted that while the Department adopted this policy in the 1980s, "the exact moment is shrouded in historical mist." See In Re Sealed Case, 310 F.3d 717, 727 (2002).

2. Institutional divide between criminal and intelligence investigations

The effect on FISA warrants or the legal restrictions on sharing intelligence information was not the only issue regarding sharing intelligence information with criminal investigators. Agents conducting intelligence investigations are generally wary about the impact of sharing intelligence information with prosecutors and criminal investigators. They expressed concerns about potential harm that disclosure would have on intelligence sources and methods, and the damage that such disclosure would have on future collection of intelligence information. Intelligence collection is dependent upon secrecy; investigators often rely upon clandestine sources or surveillance techniques that are rendered useless if they are exposed. In addition, most of the information collected is classified and cannot be made public. In contrast, criminal investigations are usually intended to result in a prosecution, which may require the disclosure of information about the source of evidence relied upon by the government. Thus, intelligence investigators' need to protect secret sources and methods may be at odds with criminal investigators' use of the information derived from those sources and methods.

3. The Ames case and concerns about the primary purpose standard

In February 1994, CIA employee Aldrich Ames was arrested on various espionage charges. The FBI pursued an investigation regarding Ames that involved several certifications to the FISA Court that the purpose of electronic surveillance was for intelligence purposes. At the time of the ninth certification in the Ames case, Richard Scruggs, the new head of OIPR, was concerned that no guidelines governed the contacts between the Criminal Division and the FBI that were permitted in intelligence investigations. Scruggs raised concerns with the Attorney General that the primary purpose requirement and FISA statute had been violated by the extensive contacts between the Criminal Division and the FBI in the Ames investigation.

To address these concerns about coordination between the Criminal Division and the FBI in intelligence investigations, in 1994 Scruggs proposed amending the Attorney General's FCI Guidelines to require that any questions in intelligence investigations relating to criminal conduct or prosecutions had to be raised first with OIPR, and that OIPR would decide whether and to what

extent to involve the Criminal Division and the USAO in the intelligence investigation. Scruggs' proposal also prohibited the FBI from contacting the Criminal Division or a USAO without permission from OIPR.

In one memorandum, Scruggs described this separation of criminal and intelligence investigations as a wall: "The simple legal response to parallel investigations is a 'Chinese Wall' which divides the attorneys as well as the investigators." Scruggs' use of the term "Chinese wall" is the first reference we found to the term "wall" in connection with separating intelligence and criminal investigations. In another memorandum discussing his proposal, Scruggs wrote that the goal of the changes was "not to prevent discussions with the Criminal Division" but "to regulate them so as to place the Department in the best possible legal posture should prosecution be undertaken." In addition, he wrote that the goal was to develop "a simple mechanism" to maintain the legal distinction between criminal investigations and intelligence operations.

Scruggs' proposal generated considerable controversy within the Department and the FBI. The Criminal Division and the FBI wrote position papers opposing the proposal. Although the Criminal Division and the FBI both agreed that some formal procedures were necessary to guard against abuses in the use of FISA and to rebut unwarranted claims of abuse, they argued that allowing OIPR to decide when prosecutors could be consulted was unnecessary and unduly burdensome, and would deter useful and productive contacts between investigators and prosecutors.[33] The Criminal Division also argued that it was "imperative" for any procedures to "allow for potential criminal prosecutions to be protected through early evaluation and guidance" and advocated continuing the requirement that the Criminal Division had to be advised any time the FBI uncovered evidence of federal criminal activity in the course of an intelligence investigation.

Also in response to Scruggs' proposal, the Executive Office for National Security, which was located in the Deputy Attorney General's Office, sought an opinion from the Office of Legal Counsel (OLC) whether a search under

---

[33] The FBI agreed, however, that the rule preventing contact with a United States Attorney's Office without approval from the Criminal Division and OIPR should remain. The FBI stated that "the requisite sensitivity to these concerns and experience with treading this fine line will often be absent" in U.S. Attorney's Offices.

FISA could be approved "only when the collection of foreign intelligence [was] the 'primary purpose' of the search or whether it suffic[ed] that the collection of foreign intelligence [was] one of the purposes." In a memorandum that was circulated in draft in mid-January 1995, OLC concluded that while courts had adhered to – and were likely to continue to adhere to – the "primary purpose" test with regard to FISA information, the courts had shown great deference to the government in challenges to evidence gathered through intelligence searches that was used in criminal prosecutions. OLC opined that some involvement of prosecutors could be permitted to be involved with the FISA searches without running an "undue risk" of having evidence suppressed, but that there were "few bright line rules" for discerning when a "'primarily' intelligence search becomes a 'primarily' criminal investigation search." OLC wrote, "[I]t must be permissible for prosecutors to be involved in the searches at least to the extent of ensuring that the possible criminal case not be prejudiced." At the end of its opinion, OLC recommended that "an appropriate internal process be set up to insure that FISA certifications are consistent with the 'primary purpose' test."

4. The 1995 Procedures

a. Creation of the 1995 Procedures

In late December 1994, at the direction of Deputy Attorney General Jamie Gorelick, the Executive Office for National Security convened a working group to resolve the dispute between OIPR and the FBI and the Criminal Division concerning contacts between the FBI and the Criminal Division. The Criminal Division, OIPR, the FBI, OLC, and the Executive Office for National Security participated in the group. As a result of discussions within the working group, on February 3, 1995, the Executive Office for National Security circulated draft procedures for contacts between the FBI and prosecutors. The draft procedures, "Procedures for Contacts Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations," were transmitted on April 12, 1995, by the Executive Office for National Security through the Deputy

Attorney General to the Attorney General for approval and implementation.[34] The Attorney General signed and issued the procedures on July 19, 1995. These procedures became known as "the 1995 Procedures."

b. Description of the 1995 Procedures

In general, the 1995 Procedures rejected OIPR's original proposal of giving it the sole authority to decide when FBI agents could consult with Criminal Division prosecutors on an intelligence investigation. However, the 1995 Procedures gave OIPR formal oversight over contacts between the FBI and the Criminal Division in intelligence cases, and the procedures formalized restrictions on the extent that Criminal Division prosecutors could be involved in intelligence investigations. The procedures applied to intelligence

---

[34] At the time these draft procedures were being discussed, the FBI's New York Field Office was conducting at least two significant criminal terrorism investigations involving the World Trade Center bombing in 1993. Indictments had been returned in one of the cases. During the criminal investigation of these two cases, significant counterintelligence information was developed relating to foreign powers operating in the United States, and the FBI initiated a full field counterintelligence investigation. In a memorandum written to the FBI, the Southern District of New York (SDNY) USAO, OIPR, and the Criminal Division, and filed with the FISA Court on March 4, 1995, Deputy Attorney General Gorelick provided instructions for sharing information from these two terrorism investigations in the FBI's New York Field Office with intelligence investigators, and for separating the counterintelligence and criminal investigations. The memorandum stated that the procedures were designed to prevent the risk of creating an unwarranted appearance that FISA was being used to avoid the procedural safeguards that applied in criminal investigations. The memorandum, which acknowledged that the procedures went "beyond what [was] legally required," included having an Assistant United States Attorney (AUSA) not involved in the criminal cases but who was familiar with them act as "the wall" as well as ensure that information indicative of a crime obtained in the intelligence investigation was passed to the criminal agents, the USAO, and the Criminal Division. The memorandum also included several procedures to facilitate coordination and information sharing, including requiring intelligence investigators who developed information that reasonably indicated the commission of a crime to notify law enforcement agents and assigning an FBI agent involved in the criminal investigation to be assigned to the foreign counterintelligence investigation.

investigations both in which a FISA search or surveillance was being conducted and in which no FISA order had been issued.[35]

The 1995 Procedures formalized the unwritten policy that had existed since the 1980s requiring the Criminal Division, rather than the local USAO, to be consulted about intelligence investigations when questions of criminal activity or criminal prosecution arose.[36] The 1995 Procedures required that the FBI and OIPR notify the Criminal Division when "facts or circumstances [were] developed that reasonably indicate[d] that a significant federal crime [had] been, [was] being, or [might have been] committed."

In cases in which FISA surveillance was being conducted, the 1995 Procedures provided that OIPR as well as the Criminal Division had to approve an FBI field office's request to take an investigation to the USAO. Guidance

---

[35] Part A of the 1995 Procedures applied to investigations in which a FISA order had been issued, and Part B applied to those investigations in which no FISA order had been issued.

[36] However, there was an exception for the USAO in the Southern District of New York (SDNY). While the 1995 Procedures were being considered in draft, Deputy Attorney General Gorelick had recommended that they be reviewed by U.S. Attorney for the SDNY Mary Jo White. White responded that the USAOs should be on equal footing with the Criminal Division, and she recommended changes to the 1995 Procedures to achieve this, such as requiring in intelligence cases notification of a crime to both the Criminal Division and to the USAO. White argued that "[a]s a legal matter, whenever it is permissible for the Criminal Division to be in contact with the FBI, it is equally permissible for the FBI to be in touch with the U.S. Attorneys' Offices." This suggestion was unanimously rejected by the FBI, OIPR, the Criminal Division, and the Executive Office for National Security, and the exception was not included in the 1995 Procedures. However, White continued to press this issue. In a memorandum faxed to Gorelick on December 27, 1995, White argued that the Department and the FBI were structured and operating in a way that did not make maximum legitimate use of all law enforcement and intelligence avenues to prevent terrorism and prosecute terrorist acts. She asserted that the 1995 Procedures were building "unnecessary and counterproductive walls that inhibit rather than promote our ultimate objectives" and that "we must face the reality that the way we are proceeding now is inherently and in actuality very dangerous." Eventually, on August 29, 1997, the Attorney General issued a memorandum creating a special exemption for the SDNY USAO in cases in which no FISA techniques were being employed. In those cases, the FBI was permitted to notify directly the SDNY USAO of evidence of a crime, and the USAO then was required to involve the Criminal Division and OIPR.

issued by the FBI Director that accompanied the 1995 Procedures instructed FBI field offices that any potential contact with prosecutors (either the Criminal Division or requests to consult with the USAO) had to be coordinated through FBI Headquarters.

In cases in which no FISA warrant had been issued, the 1995 Procedures required that the Criminal Division decide when it was appropriate to involve the USAO in the intelligence investigation, although notice of the decision had to be given to OIPR. For example, as discussed in Chapter Four, the FBI Minneapolis Field Office opened the Moussaoui investigation as an intelligence investigation, but then wanted to seek a criminal search warrant from the USAO. Since an intelligence investigation was opened but no FISA warrant had been issued, the Minneapolis FBI needed permission – which it was required to obtain through FBI Headquarters – from the Criminal Division in order to approach the USAO for a criminal search warrant.

Under the 1995 Procedures, the Criminal Division was responsible for notifying OIPR of, and giving OIPR an opportunity to participate in, all of the Criminal Division's consultations with the FBI concerning intelligence investigations in which a FISA warrant had been obtained. In intelligence investigations where no FISA warrant had been obtained, the Criminal Division had to provide notice to OIPR of its contacts with the FBI. In both types of cases, the FBI was required to maintain a log of all its contacts with the Criminal Division.

The 1995 Procedures provided that in intelligence investigations the Criminal Division could give advice to the FBI "aimed at preserving the option of a criminal prosecution," but could not "instruct the FBI on the operation, continuation, or expansion of FISA electronic surveillance or physical searches." In addition, the FBI and the Criminal Division were required to ensure that the advice intended to preserve the prosecution did not "inadvertently result in either the fact or the appearance of the Criminal Division's directing or controlling [the investigation] toward law enforcement objectives."

5. Additional restrictions on sharing intelligence information

In addition to the wall between FBI intelligence investigators and criminal prosecutors, a wall within the FBI between criminal investigations and

intelligence investigations also was created. Although it is unclear exactly when this wall within the FBI began, sometime between 1995 and 1997 the FBI began segregating intelligence investigations from criminal investigations and restricting the flow of information between agents who conducted intelligence investigations and agents who conducted criminal investigations.

As discussed above, in a position paper prepared by OIPR when the Department was considering the 1995 Procedures, OIPR recommended that the FBI be required to open separate and parallel criminal and intelligence investigations, and that the FBI place "a wall" between the two investigations by staffing the criminal investigation with FBI agents who did not have access to the intelligence investigation. This wall was intended to ensure that information from each investigation would be fully admissible in the other. OIPR proposed certain procedures for sharing information developed in the intelligence investigation that was relevant to the criminal investigation, a process that was referred to as "passing information over the wall."

The process for passing information from the intelligence investigation to the criminal investigation was that an FBI employee – usually the SSA of an international terrorism squad, the Chief Division Counsel of a field office, or an FBI Headquarters employee – would be permitted to review raw FISA intercepts or materials seized pursuant to a FISA and act as a screening mechanism to decide what to "pass" to the criminal investigators or prosecutors.

In March 1995, at the direction of the Department, the FBI established special "wall" procedures for the New York Field Office's handling of the criminal and intelligence investigations that arose out of the 1993 World Trade Center bombing. It is unclear when similar procedures were employed throughout the FBI. By 1997 OIPR was including a description of the screening or "wall" procedures in all FISA applications that were filed with the FISA Court when a criminal investigation was opened.[37] The particular

---

[37] Neither OIPR nor the FBI had any written policy requiring the inclusion of such information in FISA applications until late 2000, after the discovery of several errors in FISA applications related to information about criminal investigations and wall procedures related to those criminal investigations. These errors are discussed below in Section III, B of this chapter.

screening mechanism proposed by OIPR and approved by the Attorney General depended on how far the criminal investigation had developed.[38] If the case had recently been initiated, the SSA was usually the screener. In a case in which the USAO already was involved, others could be the screener, such as an attorney in the FBI's Office of General Counsel, OIPR, or the Attorney General. According to James Baker, the current OIPR Counsel,[39] in late 1999 the Department proposed the use of the FISA Court as "the wall." The purpose of this proposal was to ensure that the FISA Court would approve FISA applications related to threats involving the Millennium where there was a substantial nexus with related criminal cases.

6. Reports evaluating the impact of the 1995 Procedures

Although the 1995 Procedures allowed for consultation between the FBI and the Criminal Division about intelligence investigations, and in some instances required contact by the FBI with the Criminal Division, the FBI dramatically reduced its consultations with the Criminal Division after the 1995 Procedures were issued. The FBI came to understand from OIPR that any consultation with Criminal Division attorneys could result in a FISA surveillance being terminated or in OIPR not agreeing to pursue a FISA warrant. As a result, the FBI sought prosecutor input only after it was prepared to close an intelligence investigation and "go criminal."

Three reports – a July 1999 OIG report on the Department's campaign finance investigation, a May 2000 Department report on the Wen Ho Lee case, and a July 2001 General Accounting Office (GAO) report – discussed these issues and the impact of the 1995 Procedures and the wall.

---

[38] According to OIPR Counsel Baker, Attorney General Janet Reno directed the termination of certain FISA surveillances in 1998 based upon her determination that related criminal investigative activities called into question the primary purpose of the surveillance collection.

[39] Baker joined OIPR in October 1996 and became the Deputy Counsel in 1998. In May 2001, he was named Acting Counsel, and in January 2002 he became the Counsel.

a. The OIG's July 1999 report on the campaign finance investigation

The first report was the OIG's July 1999 report entitled "The Handling of FBI Intelligence Information Related to the Justice Department's Campaign Finance Investigation" (the Campaign Finance Report). The OIG report reviewed allegations that the FBI had failed to disclose certain intelligence information to Congress, FBI Director Louis Freeh, and Attorney General Janet Reno. This intelligence information related to the FBI's Campaign Finance Task Force, which had been created to investigate allegations of campaign finance violations during the 1996 presidential campaign. In connection with this review, the OIG examined issues concerning the implementation of the 1995 Procedures and the sharing of intelligence information with prosecutors and criminal investigators.

The OIG report found that the 1995 Procedures were largely misunderstood and often misapplied, resulting in undue reluctance by intelligence agents to provide information to criminal investigators and prosecutors. The report stated that "the tumult that accompanied [the] creation [of the 1995 Procedures] drastically altered the relationship between [the FBI] and prosecutors." The report found that because of OIPR's criticism of the FBI during the Ames investigation, FBI agents had become "gun shy" about conversations with Criminal Division attorneys, and the FBI's General Counsel's Office had recommended that FBI agents take a "cautious approach" by initially conferring with OIPR attorneys rather than Criminal Division attorneys. The report also noted that as a result of the FBI's concerns about OIPR's criticisms, the FBI had been "needlessly chilled" from sharing intelligence information with the Criminal Division. The report stated that the 1995 Procedures were vaguely written and provided ineffective guidance for the FBI. The report recommended that the Criminal Division, OIPR, and the FBI resolve conflicting understandings about the 1995 Procedures, and the FBI issue guidance to disabuse FBI personnel of "unwarranted concerns about contact with prosecutors."

b. The report of the Attorney General's Review Team on the Wen Ho Lee investigation

The second report addressing these issues was prepared by the Attorney General's Review Team (AGRT), which the Department established to review

the handling of the Wen Ho Lee investigation.[40] A chapter of the final AGRT report, issued in May 2000, discussed the 1995 Procedures. The AGRT report found that soon after the 1995 Procedures were implemented, OIPR prevented the FBI from contacting the Criminal Division in contravention of the requirements of the procedures. The report stated that FBI and Criminal Division officials believed that OIPR was discouraging contact by the FBI with the Criminal Division. Both FBI and Criminal Division officials believed that such contact would jeopardize existing or future FISA coverage because OIPR might not present the matter to the FISA Court or the FISA Court would deny the request if such contact occurred. The report stated, "It is clear from interviews that the AGRT has conducted that, in any investigation where FISA is employed or even remotely hoped for (and FISA coverage is *always* hoped for), the Criminal Division is considered radioactive by both the FBI and OIPR."

The AGRT report noted that OIPR Counsel Scruggs made it clear to the FBI that it was not permitted to contact prosecutors in FCI investigations without the permission of OIPR. The report stated that, as a result, former FBI Deputy Director Robert Bryant communicated to FBI agents that violating this rule was a "career stopper."

In October 1999, the AGRT made interim recommendations to the Attorney General. For example, the AGRT recommended that the FBI provide "regularly scheduled briefings" to the Criminal Division concerning FCI investigations that had the potential for criminal prosecution.

In response, in January 2000 Attorney General Reno established the "Core Group," which consisted of the FBI's Assistant Directors for counterterrorism and counterintelligence, the Principal Associate Deputy Attorney General, and the Counsel for OIPR. The FBI was supposed to provide monthly "critical case briefings" to the Core Group, and the Core Group was supposed to decide if the facts of the cases warranted notification to the Criminal Division as provided for in the 1995 Procedures. In addition, the

---

[40] The team was led by Randy Bellows, an AUSA from the Eastern District of Virginia who was experienced in FCI cases. The AGRT report, which is entitled "Final Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation," is often called "the Bellows report."

Attorney General directed the FBI to provide the Criminal Division with copies of foreign counterintelligence case memoranda summarizing espionage investigations of U.S. citizens or lawful permanent residents.

In October 2000, the Core Group was disbanded because it was believed that the briefings were duplicative of sensitive case briefings that the FBI provided to the Attorney General and the Deputy Attorney General on a quarterly basis. Around the same time a working group that had been formed months earlier in response to the interim recommendations of the AGRT report developed two decision memoranda for the Attorney General's approval, one in October 2000 and one in December 2000. The memoranda included several options for addressing the FBI's lack of notification to the Criminal Division regarding evidence in intelligence investigations of significant federal crimes and the lack of coordination with the Criminal Division, and they delineated the type and extent of advice the Criminal Division could provide the FBI. The December 2000 memorandum also described a strategy for presenting new procedures for coordination between intelligence and law enforcement to the FISA Court, and it discussed the possibility of an appeal to the FISA Court of Review if the FISA Court rejected the new coordination procedures. Although the Criminal Division, OIPR, and the FBI reached an agreement on steps to liberalize information sharing, the components could not agree on what kind of advice by the Criminal Division to the FBI was permissible. The Attorney General never issued or signed either memorandum.

c. The GAO report

In the third report, the GAO reviewed the policies, procedures, and processes for coordinating FBI intelligence investigations where criminal activity was indicated. In its July 2001 report, the GAO found that the FBI had little contact with the Criminal Division about intelligence investigations because of the FBI and OIPR's concern about the potential for "rejection of the FISA application or the loss of a FISA renewal" or "suppression of evidence gathered using FISA tools." See "FBI Intelligence Investigations: Coordination within Justice on Counterintelligence Criminal Matters is Limited," GAO-01-780, July 2001. The GAO report recommended, among other things, that the Attorney General establish a policy and guidance clarifying the expectations regarding the FBI's notification of the Criminal Division about potential criminal violations arising in intelligence

investigations. According to the GAO report, while there were some improvements in the coordination between the FBI and the Criminal Division after the remedial actions in response to the AGRT report were implemented, coordination impediments remained.

B. FISA Court's concern about accuracy of FISA applications

1. Errors in FISA applications

Around the time of these two reviews on problems of coordinating criminal and intelligence information, the FISA Court imposed additional restrictions on the passing of intelligence information to criminal investigators. The FISA Court took this action after it learned in 2000 and 2001 of errors in approximately 100 FISA applications that had been filed with the Court.[41] Approximately 75 of the errors were contained in FISA applications relating to targets with connections to a particular terrorist organization, which we will call "Terrorist Organization No. 1," and the other errors were contained in FISA applications relating to a different terrorist organization, which we will call "Terrorist Organization No. 2."

In the summer of 2000, OIPR first learned of the errors in several FISA applications related to Terrorist Organization No.1. OIPR verbally notified the FISA Court of the errors and, together with FBI Headquarters employees, conducted a review of other FISA applications involving Terrorist Organization No. 1 that had been submitted since July 1997. In September and October 2000, OIPR filed two pleadings with the FISA Court advising of errors in approximately 100 FISA applications related to Terrorist Organization No. 1.

---

[41] As discussed in detail below, FISA applications were submitted by field offices to FBI Headquarters for preparation of the documentation that would be presented to OIPR for finalization and submission to the FISA Court. The documentation prepared by FBI Headquarters and finalized by OIPR often was reviewed or edited by different persons, including an SSA, IOS, Unit Chief, and a National Security Law Unit attorney. The documentation included an affidavit signed by the SSA at FBI Headquarters containing the facts in support of the FISA warrant. The errors arose in these SSA affidavits.

Many of these errors in the FISA applications involved omissions of information or misrepresentations about criminal investigations on the FISA targets. In applications where criminal investigations were identified, inaccurate information was presented in FISA applications about the "wall" procedures to separate the criminal investigation from the intelligence investigation. For example, the description of the wall procedures in the majority of FISA applications involving Terrorist Organization No. 1 stated that the FBI New York Field Office had separate teams of agents handling the criminal and intelligence investigations. While different agents were assigned to the criminal and intelligence investigations, they were not kept separate from each other. Instead, the criminal agents worked on the intelligence investigation, and the intelligence agents worked on the criminal investigation. This meant that, contrary to what had been represented to the FISA Court, agents working on the criminal investigation had not been restricted from the information obtained in the intelligence investigation.

2. FISA Court's new requirements regarding the wall

As a result of the FISA Court's concerns about the mistakes in the FISA applications, the FISA Court began requiring in October 2000 anyone who reviewed FISA-obtained materials or other intelligence acquired based on FISA-obtained intelligence (called "FISA-derived" intelligence[42]) to sign a certification acknowledging that the Court's approval was required for dissemination to criminal investigators. The FBI came to understand that this meant that only intelligence agents were permitted to review without FISA Court approval all FISA intercepts and materials seized by a FISA warrant, as well as any CIA and NSA intelligence provided to the FBI based on information obtained by an FBI FISA search or intercept.[43]

Because FISA-obtained information often was passed from the FBI to the NSA and the CIA, the Department asked the FISA Court whether the FBI was

---

[42] FISA-obtained information was often passed to the NSA and CIA for further use, which could result in "FISA-derived" information.

[43] As stated above, in late 1999, the Court had become the screening mechanism or "the wall" for all investigations involving FISA techniques on al Qaeda in which the FBI wanted to pass intelligence information to a criminal investigation.

also required to obtain the newly required certifications from any NSA or CIA employees who reviewed the FISA-obtained material. The Court exempted the NSA and CIA from the certification, but required that the two agencies note on any intelligence shared with the FBI if it was FISA-derived. According to the NSA, when made aware of this requirement, it reported to the Department that, in the interest of providing as much intelligence as quickly as possible to the FBI, the NSA would place a caveat on all counterterrorism-related intelligence provided to the FBI. The caveat indicated that if the FBI wanted to pass NSA intelligence to criminal investigators, it had to involve the NSA General Counsel's Office to determine whether the information was in fact FISA-derived. According to the NSA, the other alternative would have been to slow the dissemination while the NSA checked whether the intelligence was derived from a FISA.[44]

The caveat language used by the NSA stated: "Except for information reflecting a direct threat to life, neither this product nor any information contained in this product may be disseminated to U.S. criminal investigators or prosecutors without prior approval of NSA. All subsequent product which contains information obtained or derived from this product must bear this caveat. Contact the Office of General Counsel of NSA for guidance concerning this caveat."[45]

---

[44] This was not the first caveat on dissemination of NSA information. In late 1999, Attorney General Reno authorized a warrantless physical search under authority granted to the Attorney General by Section 2.5 of Executive Order 12333, unrelated to FISA. The Attorney General directed that the fruits of the physical search could not be disseminated to any criminal prosecutors or investigators until copies of the information were provided to OIPR and the approval of the Attorney General had been obtained. Questions were raised about dissemination of NSA's information based upon the fruits of a Section 2.5 search. The NSA – after working with OIPR to determine what language to use -- decided to put a caveat on all of its Bin Laden related reporting to the FBI indicating that further dissemination to law enforcement entities could not occur without approval from OIPR.

[45] In Chapter Five, the chapter about Hazmi and Mihdhar, we discuss the separation of criminal investigators from intelligence investigators and the requirement that NSA information be reviewed by the NSA to determine whether it was FISA-derived or otherwise subject to limited dissemination. We describe how these restrictions affected the FBI's ability to share important intelligence information. For example, in early summer 2001 an FBI Headquarters IOS met with New York criminal agents who were working on the FBI's (continued)

3. Additional FISA errors and DOJ OPR's investigation

The Deputy Attorney General's Office referred to the DOJ Office of Professional Responsibility (OPR) a memorandum prepared by OIPR regarding the errors in the approximately 75 Terrorist Organization No. 1-related FISA applications that had been raised to the FISA Court. In November 2000, OPR opened an investigation to determine whether any FBI employees had committed misconduct in connection with these errors.

In March 2001, OIPR also became aware of an error in a FISA application related to Terrorist Organization No. 2. The error concerned the description of the wall procedures in several FBI field offices. This description also had been used in 14 other applications related to Terrorist Organization No. 2. After the FISA Court learned of these errors, it stated that it would no longer accept any FISA application in which the supporting affidavit was signed by the SSA who had presented that Terrorist Organization No. 2 FISA application to the Court.

To address the issue of the accuracy of the information in the FISA affidavits, FBI ITOS managers began requiring that FISA affidavits contain certain information, such as the signature of the field office SSA and any AUSA involved in the case indicating that they had read the affidavit and agreed with the facts as they were written. In April 2001, the entire FBI Counterterrorism Division was instructed to comply with these procedures. On May 18, 2001, the Attorney General issued additional instructions to improve the accuracy of FISA affidavits, including requiring direct communication between OIPR attorneys and the field office on whose behalf the FISA application was being prepared and establishing a FISA training program at the FBI's training academy in Quantico, Virginia. In addition, the Attorney

---

(continued)
Cole investigation. During this meeting, they discussed certain information obtained from the CIA about Mihdhar. Although the IOS had information from the NSA about Mihdhar, the IOS did not reveal this information to the FBI criminal agents at the meeting because it had not yet been approved for dissemination by the NSA. In addition, in August 2001, once the FBI opened an intelligence investigation to locate Mihdhar, the same IOS and a New York criminal agent involved in the earlier meeting discussed and disagreed about whether a criminal agent would be permitted to participate in the intelligence investigation trying to locate Mihdhar or to participate in any interview with Mihdhar.

General asked OPR to expand its investigation to include a review of the errors made in FISA applications related to Terrorist Organization No. 2.

OPR's report, which was issued on May 15, 2003, concluded that "none of the errors in the [Terrorist Organization No. 1] and [Terrorist Organization No. 2] related FISA applications were the result of professional misconduct or poor judgment by the attorneys or agents who prepared or reviewed them." The report concluded that "a majority of the errors were the result of systemic flaws in the process by which those FISA applications were prepared and reviewed." These systemic flaws included, among other things, a lack of a formal training program for attorneys in OIPR or agents at the FBI to learn about the FISA application process, a lack of policies or rules regarding the required content of FISA applications, and a lack of resources for handling FISA applications.

C. Deputy Attorney General Thompson's August 2001 memorandum

On August 6, 2001, Deputy Attorney General Larry Thompson issued a memorandum to the Criminal Division, OIPR, and the FBI regarding the Department's policies governing intelligence sharing and establishing new policy. It stated that the 1995 Procedures and the additional 2000 procedures remained in effect. The memorandum stated that "the purpose of this memorandum is to restate and clarify certain important requirements imposed by the 1995 Procedures, and the [January 2000 measures issued in response to the AGRT report], and to establish certain additional requirements."

The memorandum reiterated the requirement that the Criminal Division had to be notified when there were facts or circumstances "that reasonably indicate that a significant federal crime has been, is being or may be committed." The memorandum emphasized the notification was mandatory and that the "reasonable indication" standard was "substantially lower than probable cause."

In addition, the memorandum stated that the FBI was required to have monthly briefings with the Criminal Division on all investigations that met the notification standards. The memorandum added that the Criminal Division should identify the investigations about which it needed additional information, and the FBI was required to provide this information. The memorandum did

not address the issue of the type of advice that was permissible by Criminal Division attorneys to the FBI.

D. The impact of the wall

The actions of the Department, including OIPR, the implementation of the 1995 Procedures, the additional requirements created by the FISA Court, and the OPR investigation had several effects on the handling of intelligence and criminal investigations. First, witnesses told the OIG that the concerns of the FISA Court, the banning of the SSA from the FISA Court, the OPR investigation, and the additional requirements for sharing information imposed by the FISA Court contributed to a climate of fear in ITOS at FBI Headquarters. SSAs and IOSs at FBI Headquarters were concerned about becoming the subject of an OPR investigation and the effect that any such investigation would have on their careers.

They said they were concerned not only about the accuracy of the information they provided to the Court, but also about ensuring that intelligence information was kept separate from criminal investigations. A former ITOS Unit Chief and long-time FBI Headquarters SSA told the OIG that the certification requirement was referred to as "a contempt letter." He explained that FBI employees began fearing that they would lose their jobs if any intelligence information was shared with criminal investigators.

Second, the restrictions imposed by the FISA Court – the requirement that anyone who received intelligence sign the certification and the screening procedures applicable to both FISA-obtained and FISA-derived material – created administrative hurdles for the FBI in handling intelligence information. For example, the new requirements were imposed in December 2000, just two months after the bombing of the *U.S.S. Cole*, and during the time the FBI was actively pursuing its criminal investigation. Given the new requirements, the FBI employed several IOSs on the Cole investigation just to track all of the required certifications.

Consistent with the conclusions of the AGRT report, employees at FBI Headquarters and in the Minneapolis Field Office who we interviewed told us that before September 11, 2001, there was a general perception within the FBI that seeking prosecutor input or taking any criminal investigative step when an intelligence investigation was open potentially harmed the FBI's ability to

obtain, maintain, or renew a FISA warrant. FBI Headquarters employees described cases in which OIPR required that electronic surveillance obtained under FISA be "shut down" and that the FBI "go criminal" because permission had been requested to approach the USAO or because some other criminal step had been taken. In addition, FBI attorneys told the OIG that, in their experience, OIPR would not consider applying for a FISA warrant in a case in which OIPR determined that there was "too much" criminal activity.

OIPR Counsel Baker told the OIG that the primary concern of the FISA Court was the direction and control of the intelligence investigation by prosecutors, not sharing of intelligence information with law enforcement agents. Baker stated that the FISA Court had approved FISA applications in which there was extensive interaction between prosecutors and FBI agents, provided that OIPR was present during the interactions, there was a separation between the prosecutors and intelligence investigators, and that the FISA Court was apprised of the FBI's intended use of the FISA information.

E. Changes to the wall after September 11, 2001

Shortly after the September 11, 2001, terrorist attacks, the Department proposed lowering the wall between criminal and intelligence information by changing the language in the FISA statute from "the purpose" of the surveillance or search (for the collection of foreign intelligence information) to only "a purpose."[46] In October 2001, the Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act (the USA PATRIOT Act or the Patriot Act) was enacted, which changed the requirement from "the purpose" (for obtaining foreign intelligence) to "a significant purpose." Pub. L. No. 107-56, 115 Stat. 272, Section 218. The Patriot Act also specified that federal officers who conduct electronic surveillance or searches to obtain foreign intelligence information may consult

---

[46] The Department had been considering seeking this change to FISA prior to September 11. In August 2001, the Office of the Deputy Attorney General asked the Office of Legal Counsel (OLC) for advice on whether FISA could be amended by Congress to require that the collection of foreign intelligence information be "a purpose" of a FISA warrant rather than "the purpose." That request was under review by OLC on September 11, 2001.

with federal law enforcement officers to coordinate their efforts to investigate and protect against actual or potential attacks, sabotage, or international terrorism. Id. at Section 504.

Although the Patriot Act amendments to FISA expressly provided for the consultation and coordination between prosecutors and FBI intelligence investigators, in November 2001 the FISA Court issued an order requiring that the 1995 Procedures, as revised by Attorney General Reno's January 2000 changes and the August 2001 Thompson memorandum, be applied in all cases before the FISA Court.

In March 2002, the Attorney General issued new guidelines on intelligence sharing procedures that superseded the 1995 Procedures. The 2002 Procedures effectively removed "the wall" between intelligence and criminal investigations. The 2002 Procedures explained that since the Patriot Act allowed FISA to be used for a "significant purpose" rather than the primary purpose of obtaining foreign intelligence, FISA could "be used primarily for a law enforcement purpose, as long as a significant foreign intelligence purpose remain[ed]." (Emphasis in original.)

The 2002 Procedures also directed that the Criminal Division and OIPR shall have access to – and that the FBI shall provide – all information developed in full field foreign intelligence and counterintelligence investigations, particularly information that is necessary to the ability of the United States to investigate or protect against foreign attack, sabotage, terrorism, and clandestine intelligence activities; and information that concerns any crime which has been, is being, or is about to be committed. The 2002 Procedures provided that USAOs should receive information and engage in consultations to the same extent as that provided for the Criminal Division.

In addition to these information sharing requirements, the 2002 Procedures provided that intelligence and law enforcement officers may exchange a "full range of information and advice" concerning foreign intelligence and foreign counterintelligence investigations, "including information and advice designed to preserve or enhance the possibility of a criminal prosecution." The 2002 Procedures noted that this extensive coordination was permitted because the Patriot Act provided that such coordination shall not preclude the government's certification of a significant foreign intelligence purpose for the issuance of a warrant by the FISA Court.

The Department immediately tested the new 2002 Procedures with the FISA Court. In an opinion issued on May 17, 2002, the FISA Court accepted the information-sharing provisions of the new Procedures. However, the FISA Court rejected the Department's position that criminal prosecutors should be permitted to have a significant role in FISA surveillances and searches from start to finish. See In Re All Matters Submitted to Foreign Intelligence Surveillance Court, 218 F.Supp.2d 611 (2002). The Department appealed the Court's ruling to the Foreign Intelligence Surveillance Court of Review, the appellate court for the FISA Court. This was the first appeal ever to the FISA Court of Review.

The Court of Review rejected the FISA Court's findings, as well as the 1995 Procedures and the "primary purpose standard" that had been applied before the Patriot Act revision. See In Re Sealed Case, 310 F.3d 717 (2002). The Court of Review concluded that the restrictions of the wall imposed by the Department and the FISA Court were never required by FISA or the Constitution.[47] The Court ruled that FISA permitted the use of intelligence in criminal investigations, and that coordination between criminal prosecutors and intelligence investigators was necessary for the protection of national security. The Court concluded that while the FBI had to certify that the purpose of the FISA surveillance was to obtain foreign intelligence information, FISA did not preclude or limit the use of intelligence information in a criminal prosecution. The Court wrote, "[E]ffective counterintelligence, we have learned, requires the wholehearted cooperation of all the government's personnel who can be brought to the task." Id. at 743.

IV. The process for obtaining a FISA warrant

In this section, we describe the legal and procedural requirements for obtaining a FISA warrant prior to September 11, 2001, focusing on the requirement for a warrant to conduct a physical search like the warrant that the

---

[47] The Court of Review noted, "We certainly understand the 1995 Justice Department's effort to avoid difficulty with the FISA court, or other courts; and we have no basis to criticize any organization of the Justice Department that an Attorney General desires." Id. at 727 n. 14.

FBI's Minneapolis Field Office sought in the Moussaoui investigation, which we discuss in detail in Chapter Four.

A. Legal requirements for a FISA warrant

As noted above, FISA allows the FBI to conduct electronic surveillance and physical searches in connection with counterespionage and counterterrorism investigations. Rather than showing that the subject of the surveillance or the physical search is potentially connected to a crime, the FBI must show that there is probable cause to believe that the subject of the surveillance or search is an "agent" of a "foreign power." With respect to a warrant for a physical search, the FBI also must show that there is probable cause to believe that the property to be searched is owned, used, possessed by, or in transit to or from an "agent of a foreign power" or "a foreign power." 50 U.S.C. § 1824(a)(3).

1. Agent of a foreign power

"Foreign power" as defined in the FISA statute has several meanings, most of which pertain to the governance of a foreign nation, such as "a foreign government or any component thereof, whether or not recognized by the United States" and "an entity that is directed and controlled by a foreign government or governments." 50 U.S.C. § 1801(a)(1) & (2). The definition most applicable in the Moussaoui investigation is "a group engaged in international terrorism or activities in preparation therefor." 50 U.S.C. § 1801(a)(4). With respect to terrorism, before September 11, 2001, foreign powers that were used in requests for FISA warrants to the FISA Court included foreign governments as well as terrorist organizations not controlled by any foreign government, such as al Qaeda and Hizbollah.

Whether a terrorist organization qualified as a "foreign power" under the FISA statute depended upon the intelligence developed about the group and its activities, and whether the FISA Court was convinced that the government had proven that the entity existed and was engaged in international terrorist activities. In practice, once the FBI developed the necessary intelligence about the existence of a terrorist organization, a particular subject was used as a "test subject" for pleading to the FISA Court that the organization was a foreign power. Although not dispositive, FISA applications might reference the fact

that the State Department had designated an entity as a "foreign terrorist organization" (FTO).[48]

An "agent" of a foreign power also has several definitions in the statute. An agent can be a person who has an official connection to a foreign power, such as an employee of a foreign government or an official member of a terrorist organization. With respect to terrorism, an agent can be anyone who engages in international terrorism (or in activities that are in preparation for international terrorism) "for or on behalf of a foreign power." 50 U.S.C. § 1801(b)(2)(C).

Aside from stating that a person must be acting "for or on behalf of" a foreign power, the FISA statute does not further define when a person is an "agent." The legislative history of FISA states that there must be "a nexus between the individual and the foreign power that suggests that the person is likely to do the bidding of the foreign power," and that there must be a "knowing connection" between the individual and the foreign power. H.R. 7308, 95th Congress, 2d Session, Report 95-1283, Pt. 1, p. 49, 44 (June 8, 1978). The legislative history also states that more than evidence of "mere sympathy for, identity of interest with, or vocal support for the goals" of a terrorist organization is required to establish agency between the group and the potential subject. Id. at p. 42. The Attorney General's FCI Guidelines in effect in 2001 stated in the definition section that determining whether an individual is acting "for or on behalf of a foreign power" is based on the extent

---

[48] FTOs are foreign entities that are designated as terrorist organizations by the Secretary of State in accordance with the Antiterrorism and Effective Death Penalty Act, signed into law in April 1996. The criteria for this designation include: that the entity is a foreign organization, that the organization is engaged in terrorist activity, and that the organization's terrorist activity must threaten the security of U.S. nationals or the national security of the United States. FTO designations expire automatically after two years but may be redesignated. It is unlawful for anyone to assist an FTO, representatives and members of FTOs are not admissible into the United States, and U.S. financial institutions that become aware of possession of funds of an FTO must report this information to the government. The first 30 FTO designations were made in October 1997. As of March 2004, 37 FTOs were on the State Department list, including al Qaeda, Ansar al-Islam, and the Revolutionary Armed Forces of Columbia.

to which the foreign power is involved in controlling, leading, financially supporting, assigning or disciplining the individual.

2. The application filed with the FISA Court

To obtain an order from the FISA Court authorizing either electronic surveillance or a physical search, the FBI – through DOJ OIPR – submits to the FISA Court an application containing three documents. The first document, labeled "application," is a court pleading that contains the government's specific request for a FISA warrant and includes the required approval by the Attorney General or the Deputy Attorney General. See 50 U.S.C. § 1804(a) (electronic surveillance) and § 1823(a) (physical search). The second document is a certification by the FBI Director or other Executive Branch official that the information sought is foreign intelligence information and that the information cannot reasonably be obtained by normal investigative techniques. At the time of the Moussaoui investigation, as discussed above, the certification also had to contain a statement that the purpose of the search or surveillance was to obtain foreign intelligence information.[49] See 50 U.S.C. § 1804(a)(7) (electronic surveillance) and § 1823(a)(7) (physical search).

The third required document is an affidavit signed by an SSA from FBI Headquarters, which satisfies the FISA statute's requirement that the application be made "by a Federal officer in writing upon oath or affirmation." 50 U.S.C. § 1804(a) (electronic surveillance) and § 1823(a) (physical search). The affidavit must contain "a statement of the facts and circumstances relied upon by the applicant to justify his belief" that the foreign power identified in the application is in fact a foreign power and that there are sufficient connections between the foreign power and the individual targeted to establish that the individual is acting as an agent of the foreign power. Id. With respect to a physical search, the affidavit also must show that the property to be searched contains foreign intelligence information, and the property to be

---

[49] As previously discussed, the Patriot Act amended this section of the FISA statute to require that the certification state that "a significant purpose" of the surveillance or search is to obtain foreign intelligence information.

searched is owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power. 50 U.S.C. § 1823(a)(4).[50]

The FISA statute also provides that in order for a judge to issue an order approving the FISA application, the judge 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." 50 U.S.C. § 1805(3).

B. Assembling an application for submission to the FISA Court

Prior to September 11, 2001, the FISA application process involved several layers of review and approval at FBI Headquarters and at OIPR before presentation to the FISA Court. The process began when the field office submitted an EC or letterhead memorandum (LHM) to FBI Headquarters setting forth the supporting evidence for the FISA warrant.[51] An SSA and IOS in FBI Headquarters worked with the field office in reviewing, editing, and finalizing the LHM. An NSLU attorney reviewed, edited, and approved the LHM, then obtained several ITOS management approvals before sending the request to OIPR for consideration. Using the information provided in the LHM, an OIPR attorney drafted the FISA application and other required documents, which were reviewed in draft by the OIPR attorney's supervisor. The documentation drafted by OIPR was provided to the SSA, IOS, and NSLU attorney for their review before being finalized by the OIPR attorney and filed with the FISA Court. This process normally took several months to complete, although we were told a FISA warrant could be obtained in a matter of several hours or a few days if needed.

We describe below in more detail each step in the process, with special attention to the role of each person involved in the process.

---

[50] OIPR also submits to the FISA Court a draft order or orders for the FISA judge's completion and signature.

[51] An LHM is a memorandum on FBI letterhead stationery that is used to communicate to the Attorney General, other Department officials, or persons or agencies outside the FBI.

1. Investigation and LHM prepared by field office

An application for a FISA warrant normally originated from the investigative work conducted by a field office. During the investigation, the field office typically developed information about the subject of the investigation by checking FBI indices and files, reviewing publicly available records, and inquiring with domestic and foreign law enforcement and intelligence agencies – such as the CIA and NSA – about the subject. In addition, the field office could conduct other investigative activities. The field office also could obtain the subject's records of telephone calls, computer transactions, and financial information through National Security Letters (NSLs).[52] This phase of collecting information can last anywhere from several days to several months.

If a field office wanted to obtain a FISA warrant and thought it had sufficient information to support a FISA warrant, the field office prepared an LHM setting forth as specifically as possible the supporting information. The LHM was sent to the appropriate unit at FBI Headquarters, where it was assigned to a particular SSA for handling.

2. Role of SSAs and IOSs at FBI Headquarters

At the time of the Moussaoui investigation in August 2001, once the LHM was received in FBI Headquarters by the appropriate SSA, that SSA was responsible for ensuring that the FISA request was adequately supported and complete before it was presented to OIPR. To do this, the SSA – working in conjunction with the assigned IOS – reviewed the documentation to assess whether it contained sufficient information for a FISA or whether there were questions that would have to be answered before the request could be

---

[52] NSLs are issued in intelligence investigations to obtain telephone and electronic communications records from telephone companies and internet service providers (pursuant to the Electronic Communications Privacy Act, or ECPA, 18 U.S.C. § 2709), records from financial institutions (pursuant to the Right to Financial Privacy Act, 12 U.S.C. § 3414(a)(5)), and information from credit bureaus (pursuant to the Fair Credit Reporting Act, 15 U.S.C. §§ 1681u and 1681v). They do not require approval of a court before issuance by the FBI. Prior to September 11, the process for issuing NSLs could take several months. We discuss this issue in Chapter Four of the report.

completed. The SSA also assessed whether the appropriate foreign power was being pled and whether there was sufficient information connecting the subject to the foreign power.

The SSA and the IOS communicated with the field office directly about any problems or for additional information. In problematic cases, the SSA would consult with an NSLU attorney for advice and suggestions.

The SSA and the IOS used the documentation submitted by the field office and often edited the document. In some instances, the FISA request was completely rewritten, and in other instances few changes were made.

With respect to the information supporting the existence of the foreign power, the SSA or IOS typically inserted language used in other FISA applications involving the same foreign power. If the SSA or IOS acquired additional information to support the application, such as information indicating connections between the subject and the foreign power, that information was also included in the LHM.

At the time of the Moussaoui investigation, the SSA would normally review the edited version of the LHM with the field office to ensure the factual accuracy of the LHM.[53] Once the field office and the SSA agreed on the final version of the LHM, the SSA sought review and approval by an NSLU attorney and finally obtained the appropriate signatures within FBI Headquarters management, such as the signatures of the Unit and Section Chiefs. This editing process could last from several days to several months.

---

[53] Such consultations with the field office about edits arose primarily because of the problems the FBI had encountered with the FISA Court in the fall of 2000 and spring of 2001 over inaccuracies in the affidavits signed by SSAs and filed with the FISA Court. In March 2001, the FBI adopted procedures requiring the SSA at FBI Headquarters handling a FISA request to review OIPR's draft affidavit with the field office to ensure the factual accuracy of the affidavit before it was filed with the FISA Court. Because of these requirements and other concerns about the accuracy of the affidavits, SSAs spent more time than they had in the past discussing drafts of FISA documents with field offices.

3. Role of NSLU attorneys

At the time of the Moussaoui investigation in August 2001, two attorneys in the National Security Law Unit (NSLU) of the FBI's Office of the General Counsel were assigned full-time to counterterrorism matters.[54] No attorney was assigned responsibility for a particular FISA request from beginning to end.

The two NSLU attorneys assigned to counterterrorism matters had two functions with respect to FISA requests submitted by field offices. First, they functioned in an advisory capacity. The SSA would consult with an NSLU attorney if a question or problem arose or if the SSA needed legal advice. NSLU attorneys also were consulted when there was a disagreement between the field office and FBI Headquarters about a particular issue, such as whether there was sufficient support for a FISA warrant. SSAs often discussed with NSLU attorneys whether the threshold of probable cause had been met for supporting that a subject was an agent of a foreign power. The former head of the NSLU told the OIG, however, that in "slam dunk" cases, FBI Headquarters would deal directly with OIPR without consulting an NSLU attorney.

The second function of NSLU attorneys with respect to FISA requests was to review the LHM once it was finalized and to advise whether they believed OIPR would accept the LHM as having sufficient evidence to obtain a FISA warrant. If the NSLU attorney did not believe that the LHM contained sufficient evidence, the NSLU attorney would advise the SSA what additional information was needed and make suggestions about how the additional information could be acquired. Once the LHM was finalized and approved by the NSLU attorney, the signatures of the Unit Chief and the Section Chief were obtained, and the LHM was sent to OIPR.

The NSLU attorney and the SSA also could make recommendations to the field office about how to acquire any additional information that was needed. If the field office provided additional information to support the FISA request, the LHM was revised and the FISA request was reviewed again. This process would continue until the NSLU attorney was satisfied that the

---

[54] Other NSLU attorneys primarily worked counterintelligence matters, although some of them assisted with counterterrorism matters when necessary.

standards for obtaining the FISA warrant were met. This step in the process also could last from several days to several months.

4. Role of OIPR attorneys

Once the SSA obtained the necessary FBI Headquarters approvals, the LHM and its supporting documents were provided to OIPR for preparation of the required pleadings. An OIPR attorney would review the LHM and determine whether there was sufficient evidence to obtain a FISA warrant. The OIPR attorney would consult with the FBI Headquarters SSA about any questions and would sometimes prepare a list of questions for the SSA to answer in writing. The SSA often consulted with the field office to obtain the information requested by the OIPR attorney and sometimes asked the field office to conduct additional investigation. This process also could take anywhere from several days to several months.

Once the OIPR attorney was satisfied that there was sufficient evidence to support the FISA application, an OIPR attorney prepared the draft pleadings. A supervisory attorney in OIPR would review the draft pleadings and make recommendations and revisions. The final draft was provided to the SSA and the NSLU attorney for review. After finalizing the pleadings and obtaining the signatures of the FBI Headquarters SSA who signed the affidavit, the Attorney General, and the FBI Director, the OIPR attorney filed the pleadings with the FISA Court, along with a draft order for the judge's signature. The FISA Court would then schedule a hearing, which was attended by the OIPR attorney and the SSA.

If the FISA Court approved the warrant, it issued an order authorizing the surveillance or search. Orders authorizing surveillance were for a specific period, beginning and ending on a certain day and time. The order was transmitted to the field office responsible for conducting the surveillance or search.

5. Expedited FISA warrants

In the Moussaoui investigation, the Minneapolis Field Office requested an "emergency FISA," which was a FISA that could be obtained in an

expedited manner.[55] The SSAs and NSLU attorneys we interviewed told us that what rose to the level of "expedited" depended on what the field office and ITOS management deemed to be an immediate priority. According to these witnesses, in the summer of 2001 expedited FISA requests normally involved reports of a suspected imminent attack or other imminent danger.

Although the normal processing time for a FISA application was several weeks or months, FBI Headquarters working with an NSLU attorney and OIPR could prepare an expedited FISA application for presentation to the FISA Court in a matter of several hours or days, depending on the circumstances giving rise to the expedited request.

---

[55] Although expedited FISA requests were commonly referred to as "emergency FISAs," the statute provided for an "emergency FISA" that was different from an expedited FISA. The statute stated that an emergency FISA allowed the Attorney General - *without* prior approval of the FISA Court - to authorize the execution of a search warrant or electronic surveillance if the Attorney General determined that "an emergency situation exists" and there was a "the factual basis for issuance of an order" in accordance with the statute. See 50 U.S.C. § 1805(e) (electronic surveillance) & § 1824(e) (physical search warrant). The government was required to present an application to the FISA Court with respect to any such warrantless search or electronic surveillance within 24 hours of the execution of the search or surveillance. 50 U.S.C. § 1805(e) (electronic surveillance) & § 1824(e) (physical search warrant). This type of emergency FISA rarely was used before September 11, 2001.