

Attachment A

MAY 17 2002

U.S. Foreign Intelligence
Surveillance Court

§1801(h) and §1821(4) of the Act. The Government's motion will be GRANTED, EXCEPT THAT THE PROCEDURES MUST BE MODIFIED IN PART.

The Court's analysis and findings are as follows:

JURISDICTION. Section 1803 of the FISA which established this Court provides that the Court "shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this Act." The comparable provision added when the FISA was amended to include physical searches appears in §1822(c) entitled "Jurisdiction of Foreign Intelligence Surveillance Court," and says

The Foreign Intelligence Surveillance Court shall have jurisdiction to hear applications for and grant orders approving a physical search for the purpose of obtaining foreign intelligence information anywhere in the United States under the procedures set forth in this subchapter. (emphasis added)

Examination of the text of the statute leaves little doubt that the collection of foreign intelligence information is the raison d'etre for the FISA. Starting with its title, foreign intelligence information is the core of the Act:

- foreign intelligence information is defined in §1801(e);
- minimization procedures to protect the privacy rights of Americans, defined in §1801(h), and §1821 (4), must be reasonably designed and consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
- section 1802(b) which authorizes the Government to file applications for electronic

MAY 17 2002

U.S. Foreign Intelligence
Surveillance Court

surveillance with this Court, empowers the judges of this Court to grant orders “approving electronic surveillance of a foreign power or agent of a foreign power for the purpose of obtaining foreign intelligence information.” (emphasis added);

- applications for electronic surveillance and physical search must contain a certification from a senior Executive Branch official (normally the FBI Director in U.S. person cases) that “the information sought is foreign intelligence information,” that “a significant purpose of the surveillance is to obtain foreign intelligence information,” that “such [foreign intelligence] information cannot reasonably be obtained by normal investigative techniques,” and “designates the type of foreign intelligence information being sought.” (§1804 (a)(7)) Comparable requirements apply in applications for physical searches. (§1823 (a)(7)).
- Applications for physical searches must contain a statement of the facts and circumstances relied on by the FBI affiant to justify his or her belief that the premises or property to be searched contains foreign intelligence information and a statement of the nature of the foreign intelligence information being sought. (§1823 (a)(4)(B) and §1823 (a) (6)).

Additionally, the two Presidential Executive orders empowering the Attorney General to approve the filing of applications for electronic surveillances and physical searches, and granting the FBI Director and other senior executives the power to make the certifications required under the Act, specify “the purpose of obtaining foreign intelligence information.” (emphasis added)

MAY 17 2002

U.S. Foreign Intelligence
Surveillance Court

(E.O. 12139, May 23, 1979, and E.O. 12949, February 9, 1995). Clearly this Court's jurisdiction is limited to granting orders for electronic surveillances and physical searches for the collection of foreign intelligence information under the standards and procedures prescribed in the Act¹.

SCOPE. Our findings regarding minimization apply only to communications of or concerning U.S. persons as defined in §1801(i) of the act: U.S. citizens and permanent resident aliens whether or not they are the named targets in the electronic surveillances and physical searches. Conversely, this opinion does not apply to communications of foreign powers defined in §1801(a), nor to non-U.S. persons.

METHODOLOGY. The analysis and findings in this opinion are based on traditional statutory construction of the FISA's provisions. The question before the Court involves straightforward application of the FISA as it pertains to minimization procedures, and raises no constitutional questions that need be decided. Discretion to evaluate proposed minimization procedures has been vested in the Court by the Congress expressly in the Act. (§1805(a)(4) and §1824(a)(4)). The Court's determinations are grounded in the plain language of the FISA, and where applicable, in its legislative history. The statute requires the Court to make the necessary findings, to issue orders "as requested or modified," for electronic surveillances and physical

¹ On April 17, 2002 the Government filed a supplemental memorandum of law in support of its March 7, 2002 motion. The supplemental memorandum misapprehends the issue that is before the Court. That issue is whether the FISA authorizes electronic surveillances and physical searches primarily for law enforcement purposes so long as the Government also has "a significant" foreign intelligence purpose. The Court is not persuaded by the supplemental memorandum, and its decision is not based on the issue of its jurisdiction but on the interpretation of minimization procedures.

MAY 17 2012

U.S. Foreign Intelligence
Surveillance Court

searches, as well as to “assess compliance” with minimization procedures for information concerning U.S. persons. (§1805 and §1824 of the Act).

CONSIDERATION OF THE ISSUE. Prior to May of 1979, when the FISA became operational, it was not uncommon for courts to defer to the expertise of the Executive Branch in matters of foreign intelligence collection. Since May 1979, this Court has often recognized the expertise of the government in foreign intelligence collection and counterintelligence investigations of espionage and international terrorism, and accorded great weight to the government’s interpretation of FISA’s standards. However, this Court, or on appeal the Foreign Intelligence Surveillance Court of Review having jurisdiction “to review the denial of any application,” is the arbiter of the FISA’s terms and requirements. (§1803(b)) The present seven members of the Court have reviewed and approved several thousand FISA applications, including many hundreds of surveillances and searches of U.S. persons. The members bring their specialized knowledge to the issue at hand, mindful of the FISA’s preeminent role in preserving our national security, not only in the present national emergency, but for the long term as a constitutional democracy under the rule of law.

II

We turn now to the government’s proposed minimization procedures which are to be followed in all electronic surveillances and physical searches past, present, and future. In addition to the Standard Minimization Procedures for a U.S. Person Agent of a Foreign Power that are filed with the Court, which we continue to approve, the government has submitted new

MAY 17 2002

U.S. Foreign Intelligence
Surveillance Court

supplementary minimization procedures adopted by the Attorney General and promulgated in the form of a memorandum addressed to the Director of the FBI and other senior Justice Department executives and dated March 6, 2002. (hereafter the Attorney General's memorandum or the 2002 procedures). The Attorney General's memorandum is divided into three sections entitled:

"I. INTRODUCTION AND STATEMENT OF GENERAL PRINCIPLES,"²

"II. INTELLIGENCE SHARING PROCEDURES CONCERNING THE CRIMINAL DIVISION," AND "III. INTELLIGENCE SHARING PROCEDURES CONCERNING A USAO."

The focus of this decision is sections II and III which set out supplementary procedures affecting the acquisition, retention, and dissemination of information obtained through electronic surveillances and physical searches of U.S. persons to be approved as part of the government's applications and incorporated in the orders of this Court.

Our duty regarding approval of these minimization procedures is inscribed in the Act, as is the standard we must follow in our decision making. Where Congress has enacted a statute like the FISA, and defined its terms, we are bound to follow those definitions. We cannot add to, subtract from, or modify the words used by Congress, but must apply the FISA's provisions with

²The Attorney General's memorandum of March 6, 2002 asserts its interpretation of the recent amendments to the FISA to mean that the Act can now "be used primarily for a law enforcement purpose, so long as a significant foreign intelligence purpose remains." The government supports this argument with a lengthy memorandum of law which we have considered. However, the Court has decided this matter by applying the FISA's standards for minimization procedures defined in §1801(h) and §1821(4) of the Act, and does not reach the question of whether the FISA may be used primarily for law enforcement purposes. We leave this question for another day.

fidelity to their plain meaning and in conformity with the overall statutory scheme. The FISA is a statute of unique character, intended to authorize electronic surveillances and physical searches of foreign powers and their agents, including U.S. persons. "Further, as a statute addressed entirely to 'specialists,' it must, as Mr. Justice Frankfurter observed, 'be read by judges with the minds of *** specialists'."³

The Attorney General's new minimization procedures are designed to regulate the acquisition, retention, and dissemination of information involving the FISA (i.e., disseminating information, consulting, and providing advice) between FBI counterintelligence and counter-terrorism officials on the one hand, and FBI criminal investigators, trial attorneys in the Justice Department's Criminal Division, and U.S. Attorney's Offices on the other hand. These new minimization procedures supersede similar procedures issued by the Attorney General in July 1995 (hereafter the 1995 procedures) which were augmented in January 2000, and then in August 2001 by the current Deputy Attorney General. The Court has relied on the 1995 procedures, which have been followed by the FBI and the Justice Department in all electronic surveillances and physical searches of U.S. persons since their promulgation in July 1995. In November 2001, the court formally adopted the 1995 procedures, as augmented, as minimization procedures defined in §1801(h) and §1821(4), and has incorporated them in all applicable orders and warrants granted since then.

³Cheng Fan Kwok v. Immigration and Naturalization Service, 392 U.S. 206, 88 S.Ct. 1970 (1968).

MAY 17 2002

U.S. Foreign Intelligence
Surveillance Court

The 2002 procedures have been submitted to the Court pursuant to §1804(a)(5) and §1823(a)(5) to supplement the Standard Minimization Procedures for U.S. Person Agents of Foreign Powers. Both sets of procedures are to be applied in past and future electronic surveillances and physical searches subject to the approval of this Court. Pursuant to §1805(a) and §1824(a) the Court has carefully considered the 2002 intelligence sharing procedures. The Court finds that these procedures 1) have been adopted by the Attorney General, 2) are designed to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons, and 3) are, therefore, minimization procedures as defined in §1801(h) and §1821(4).

The standard we apply in these findings is mandated in §1805(a)(4) and §1824(a)(4), which state that “the proposed minimization procedures meet the definition of minimization procedures under §101(h), [§1801(h) and §1821(4)] of the Act.” The operative language of each section to be applied by the Court provides that minimization procedures must be reasonably designed in light of their purpose and technique, and mean –

specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, [search] to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.
§1801(h)(1) and §1821(4)(A).

Thus in approving minimization procedures the Court is to ensure that the intrusiveness of foreign intelligence surveillances and searches on the privacy of U.S. persons is “consistent” with

MAY 17 2022

U.S. Foreign Intelligence
Surveillance Court

the need of the United States to collect foreign intelligence information from foreign powers and their agents.

Our deliberations begin with an examination of the first part of §1801(h) and §1821(4) involving the acquisition, retention and dissemination of U.S. person information. Most of the rules and procedures for minimization are set forth in the Standard Minimization Procedures which will continue to be applied along with the 2002 procedures, and permit exceptionally thorough acquisition and collection through a broad array of contemporaneous electronic surveillance techniques. Thus, in many U.S. person electronic surveillances the FBI will be authorized to conduct, simultaneously, telephone, microphone, cell phone, e-mail and computer surveillance of the U.S. person target's home, workplace and vehicles. Similar breadth is accorded the FBI in physical searches of the target's residence, office, vehicles, computer, safe deposit box and U.S. mails where supported by probable cause. The breadth of acquisition is premised on the fact that clandestine intelligence activities and activities in preparation for international terrorism are undertaken with considerable direction and support from sophisticated intelligence services of nation states and well-financed groups engaged in international terrorism.

The intrusiveness of the FBI's electronic surveillances and sophisticated searches and seizures is sanctioned by the following practices and provisions in the FISA:

- a foreign intelligence standard of probable cause instead of the more traditional criminal standard of probable cause;
- having to show only that the place or facility to be surveilled or searched is being

- (c) Examination of available federal, state, and local government records;
- (d) Interview of the complainant, previously established informants, and other sources of information;
- (e) Interview of the potential subject;
- (f) Interview of persons who should readily be able to corroborate or deny the truth of the allegation, except this does not include pretext interviews or interviews of a potential subject's employer or co-workers unless the interviewee was the complainant; and
- (g) Physical or photographic surveillance of any person.

The use of any other lawful investigative technique that is permitted in an inquiry shall meet the requirements and limitations of Part IV and, except in exigent circumstances, requires prior approval by a supervisory agent.

(7) Where a preliminary inquiry fails to disclose sufficient information to justify an investigation, the FBI shall terminate the inquiry and make a record of the closing. In a sensitive criminal matter, the FBI shall notify the United States Attorney of the closing and record the fact of notification in writing. Information on an inquiry which has been closed shall be available on request to a United States Attorney or his or her designee or an appropriate Department of Justice official.

(8) All requirements regarding inquiries shall apply to reopened inquiries. In sensitive criminal matters, the United States Attorney or the appropriate Department of Justice official shall be notified as soon as practicable after the reopening of an inquiry.

C. INVESTIGATIONS

(1) A **general crimes investigation** may be initiated by the FBI when facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed. The investigation may be conducted to prevent, solve, or prosecute such criminal activity.

The standard of "reasonable indication" is substantially lower than probable cause. In determining whether there is reasonable indication of a federal criminal violation, a Special Agent may take into account any facts or circumstances that a prudent investigator would consider. However, the standard does require specific facts or circumstances indicating a past, current, or future violation. There must be an objective, factual basis for initiating the investigation; a mere hunch is insufficient.

(2) Where a criminal act may be committed in the future, preparation for that act can be a current criminal violation under the conspiracy or attempt provisions of federal criminal law or other provisions defining preparatory crimes, such as 18 U.S.C. 373 (solicitation of a crime of violence) or 18 U.S.C. 2339A (including provision of material support in preparation for a terrorist crime). The standard for opening an investigation is satisfied where there is not yet a current substantive or preparatory crime, but facts or circumstances reasonably indicate that such a crime will occur in the future.

(3) The FBI supervisor authorizing an investigation shall assure that the facts or circumstances meeting the standard of reasonable indication have been recorded in writing.

In sensitive criminal matters, as defined in paragraph A(2), the United States Attorney or an appropriate Department of Justice official, as well as FBIHQ, shall be notified in writing of the basis for an investigation as soon as practicable after commencement of the investigation.

(4) The Special Agent conducting an investigation shall maintain periodic written or oral contact with the appropriate federal prosecutor, as circumstances require and as requested by the prosecutor.

When, during an investigation, a matter appears arguably to warrant prosecution, the Special Agent shall present the relevant facts to the appropriate federal prosecutor. In every sensitive criminal matter, the FBI shall notify the appropriate federal prosecutor of the termination of an investigation within 30 days of such termination. Information on investigations which have been closed shall be available on request to a United States Attorney or his or her designee or an appropriate Department of Justice official.

(5) When a serious matter investigated by the FBI is referred to state or local authorities for prosecution, the FBI, insofar as resources permit, shall promptly advise the federal prosecutor in writing if the state or local authorities decline prosecution or fail to commence prosecutive action within 120 days. Where an FBI field office cannot provide this follow-up, the SAC shall so advise the federal prosecutor.

(6) When credible information is received concerning serious criminal activity not within the FBI investigative jurisdiction, the FBI field office shall promptly transmit the information or refer the complainant to the law enforcement agencies having jurisdiction, except where disclosure would jeopardize an ongoing investigation, endanger the safety of an individual, disclose the identity of an informant, interfere with an informant's cooperation, or reveal legally privileged information. If full disclosure is not made for the reasons indicated, then whenever feasible the FBI field office shall make at least limited disclosure to the law enforcement agency having jurisdiction, and full

disclosure shall be made as soon as the need for restricting dissemination is no longer present. Where full disclosure is not made to the appropriate law enforcement agencies within 180 days, the FBI field office shall promptly notify FBI Headquarters in writing of the facts and circumstances concerning the criminal activity. The FBI shall make a periodic report to the Deputy Attorney General on such nondisclosure and incomplete disclosures, in a form suitable to protect the identity of informants.

Whenever information is received concerning unauthorized criminal activity by a confidential informant, it shall be handled in accordance with the Attorney General's Guidelines Regarding the Use of Confidential Informants.

(7) All requirements regarding investigations shall apply to reopened investigations. In sensitive criminal matters, the United States Attorney or the appropriate Department of Justice official shall be notified in writing as soon as practicable after the reopening of an investigation.

III. CRIMINAL INTELLIGENCE INVESTIGATIONS

This section authorizes the FBI to conduct criminal intelligence investigations of certain enterprises. These investigations differ from general crimes investigations, authorized by Section II, in several important respects. As a general rule, an investigation of a completed criminal act is normally confined to determining who committed that act and securing evidence to establish the elements of the particular offense. It is, in this respect, self-defining. An intelligence investigation of an ongoing criminal enterprise must determine the size and composition of the group involved, its geographic dimensions, its past acts and intended criminal goals, and its capacity for harm. While a standard criminal investigation terminates with the decision to prosecute or not to prosecute, the investigation of a criminal enterprise does not necessarily end, even though one or more of the participants may have been prosecuted.

In addition, the organization provides a life and continuity of operation that are not normally found in a regular criminal activity. As a consequence, these investigations may continue for several years. Furthermore, the focus of such investigations "may be less precise than that directed against more conventional types of crime." United States v. United States District Court, 407 U.S. 297, 322 (1972). Unlike the usual criminal case, there may be no completed offense to provide a framework for the investigation. It often requires the fitting together of bits and pieces of information, many meaningless by themselves, to determine whether a pattern of criminal activity exists. For this reason, the investigation is broader and less discriminate than usual, involving "the interrelation of various sources and types of information." Id.

Members of groups or organizations acting in concert to violate the law present a grave threat to society. An investigation of organizational activity, however, may present special problems particularly where it deals with politically motivated acts. There is "often . . . a

convergence of First and Fourth Amendment values” in such matters that is “not present in cases of ‘ordinary’ crime.” *Id.* at 313. Thus special care must be exercised in sorting out protected activities from those which may lead to violence or serious disruption of society. As a consequence, the guidelines establish safeguards for group investigations of special sensitivity, including tighter management controls and higher levels of review.

A. RACKETEERING ENTERPRISE INVESTIGATIONS

This section focuses on investigations of organized crime. It is concerned with the investigation of entire enterprises, rather than just individual participants and specific criminal acts, and authorizes investigations to determine the structure and scope of the enterprise as well as the relationship of the members.

1. Definition

Racketeering activity is any offense, including a violation of state law, encompassed by the Racketeer Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. 1961(1).

2. General Authority

- a. A racketeering enterprise investigation may be initiated when facts or circumstances reasonably indicate that two or more persons are engaged in a pattern of racketeering activity as defined in the RICO statute, 18 U.S.C. 1961(5). However, if the pattern of racketeering activity involves an offense or offenses described in 18 U.S.C. 2332b(g)(5)(B), the investigation shall be deemed a terrorism enterprise investigation and shall be subject to the standards and procedures of Subpart B of this Part in lieu of those set forth in this Subpart. The standard of “reasonable indication” is identical to that governing the initiation of a general crimes investigation under Part II.
- b. Authority to conduct racketeering enterprise investigations is in addition to general crimes investigative authority under Part II, terrorism enterprise investigative authority under Subpart B of this Part, and activities under other Attorney General guidelines addressing such matters as investigations and information collection relating to international terrorism, foreign counterintelligence, or foreign intelligence. Information warranting initiation of a racketeering enterprise investigation may be obtained during the course of a general crimes inquiry or investigation, a terrorism enterprise investigation, or an investigation under other Attorney General guidelines. Conversely, a racketeering enterprise investigation may yield information warranting a general crimes inquiry or

investigation, a terrorism enterprise investigation, or an investigation under other Attorney General guidelines.

3. Purpose

The immediate purpose of a racketeering enterprise investigation is to obtain information concerning the nature and structure of the enterprise, as specifically delineated in paragraph (4) below, with a view to the longer range objective of detection, prevention, and prosecution of the criminal activities of the enterprise.

4. Scope

- a. A racketeering enterprise investigation properly initiated under these guidelines may collect such information as:
 - (i) the members of the enterprise and other persons likely to be knowingly acting in the furtherance of racketeering activity, provided that the information concerns such persons' activities on behalf of or in furtherance of the enterprise;
 - (ii) the finances of the enterprise;
 - (iii) the geographical dimensions of the enterprise; and
 - (iv) the past and future activities and goals of the enterprise.
- b. In obtaining the foregoing information, any lawful investigative technique may be used, in accordance with the requirements of Part IV.

5. Authorization and Renewal

- a. A racketeering enterprise investigation may be authorized by the Special Agent in Charge, with notification to FBIHQ, upon a written recommendation setting forth the facts and circumstances reasonably indicating that the standard of paragraph (2)(a) is satisfied.
- b. The FBI shall notify the Organized Crime and Racketeering Section of the Criminal Division and any affected United States Attorney's office of the opening of a racketeering enterprise investigation. On receipt of such notice, the Organized Crime and Racketeering Section shall immediately notify the Attorney General and the Deputy Attorney General. In all racketeering enterprise investigations, the Chief of the Organized Crime

and Racketeering Section may, as he or she deems necessary, request the FBI to provide a report on the status of the investigation.

- c. A racketeering enterprise investigation may be initially authorized for a period of up to a year. An investigation may be continued upon renewed authorization for additional periods each not to exceed a year. Renewal authorization shall be obtained from the SAC with notification to FBIHQ. The FBI shall notify the Organized Crime and Racketeering Section of any renewal, and the Organized Crime and Racketeering Section shall immediately notify the Attorney General and the Deputy Attorney General.
- d. Investigations shall be reviewed by the SAC on or before the expiration of the period for which the investigation and each renewal thereof is authorized.
- e. An investigation which has been terminated may be reopened upon a showing of the same standard and pursuant to the same procedures as required for initiation of an investigation.
- f. In addition to the authority of Special Agents in Charge under this paragraph, the Director of the FBI, and any Assistant Director or senior Headquarters official designated by the Director, may authorize, renew, review, and reopen racketeering enterprise investigations in conformity with the standards of this paragraph.

B. TERRORISM ENTERPRISE INVESTIGATIONS

This section focuses on investigations of enterprises that seek to further political or social goals through activities that involve force or violence, or that otherwise aim to engage in terrorism or terrorism-related crimes. Like the section addressing racketeering enterprise investigations, it is concerned with the investigation of entire enterprises, rather than just individual participants and specific criminal acts, and authorizes investigations to determine the structure and scope of the enterprise as well as the relationship of the members.

1. General Authority

- a. A terrorism enterprise investigation may be initiated when facts or circumstances reasonably indicate that two or more persons are engaged in an enterprise for the purpose of: (i) furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law, (ii) engaging in terrorism as defined in 18 U.S.C. 2331(1) or (5) that involves a violation of federal criminal law,

or (iii) committing any offense described in 18 U.S.C. 2332b(g)(5)(B). A terrorism enterprise investigation may also be initiated when facts or circumstances reasonably indicate that two or more persons are engaged in a pattern of racketeering activity as defined in the RICO statute, 18 U.S.C. 1961(5), that involves an offense or offenses described in 18 U.S.C. 2332b(g)(5)(B). The standard of “reasonable indication” is identical to that governing the initiation of a general crimes investigation under Part II. In determining whether an investigation should be conducted, the FBI shall consider all of the circumstances including: (i) the magnitude of the threatened harm; (ii) the likelihood it will occur; (iii) the immediacy of the threat; and (iv) any danger to privacy or free expression posed by an investigation.

- b. Authority to conduct terrorism enterprise investigations is in addition to general crimes investigative authority under Part II, racketeering enterprise investigative authority under Subpart A of this Part, and activities under other Attorney General guidelines addressing such matters as investigations and information collection relating to international terrorism, foreign counterintelligence, or foreign intelligence. Information warranting initiation of a terrorism enterprise investigation may be obtained during the course of a general crimes inquiry or investigation, a racketeering enterprise investigation, or an investigation under other Attorney General guidelines. Conversely, a terrorism enterprise investigation may yield information warranting a general crimes inquiry or investigation, a racketeering enterprise investigation, or an investigation under other Attorney General guidelines.
- c. Mere speculation that force or violence might occur during the course of an otherwise peaceable demonstration is not sufficient grounds for initiation of an investigation under this Subpart, but where facts or circumstances reasonably indicate that a group or enterprise has engaged or aims to engage in activities involving force or violence or other criminal conduct described in paragraph (1)(a) in a demonstration, an investigation may be initiated in conformity with the standards of that paragraph. For alternative authorities see Part II relating to General Crimes Investigations and the Attorney General’s Guidelines on Reporting on Civil Disorders and Demonstrations Involving a Federal Interest. This does not limit the collection of information about public demonstrations by enterprises that are under active investigation pursuant to paragraph (1)(a) above.

2. Purpose

The immediate purpose of a terrorism enterprise investigation is to obtain information concerning the nature and structure of the enterprise as specifically delineated in paragraph (3) below, with a view to the longer range objectives of detection, prevention, and prosecution of the criminal activities of the enterprise.

3. Scope

- a. A terrorism enterprise investigation initiated under these guidelines may collect such information as:
- (i) the members of the enterprise and other persons likely to be knowingly acting in furtherance of its criminal objectives, provided that the information concerns such persons' activities on behalf of or in furtherance of the enterprise;
 - (ii) the finances of the enterprise;
 - (iii) the geographical dimensions of the enterprise; and
 - (iv) past and future activities and goals of the enterprise.
- b. In obtaining the foregoing information, any lawful investigative technique may be used, in accordance with the requirements of Part IV.

4. Authorization and Renewal

- a. A terrorism enterprise investigation may be authorized by the Special Agent in Charge, with notification to FBIHQ, upon a written recommendation setting forth the facts or circumstances reasonably indicating the existence of an enterprise as described in paragraph (1)(a). The FBI shall notify the Terrorism and Violent Crime Section of the Criminal Division, the Office of Intelligence Policy and Review, and any affected United States Attorney's office of the opening of a terrorism enterprise investigation. On receipt of such notice, the Terrorism and Violent Crime Section shall immediately notify the Attorney General and the Deputy Attorney General. In all such investigations, the Chief of the Terrorism and Violent Crime Section may, as he or she deems necessary, request the FBI to provide a report on the status of the investigation.
- b. A terrorism enterprise investigation may be initially authorized for a period of up to a year. An investigation may be continued upon renewed

authorization for additional periods each not to exceed a year. Renewal authorization shall be obtained from the SAC with notification to FBIHQ. The FBI shall notify the Terrorism and Violent Crime Section and the Office of Intelligence Policy and Review of any renewal, and the Terrorism and Violent Crime Section shall immediately notify the Attorney General and the Deputy Attorney General.

- c. Investigations shall be reviewed by the SAC on or before the expiration of the period for which the investigation and each renewal thereof is authorized. In some cases, the enterprise may meet the threshold standard but be temporarily inactive in the sense that it has not engaged in recent acts of violence or other criminal activities as described in paragraph (1)(a), nor is there any immediate threat of harm – yet the composition, goals and prior history of the group suggest the need for continuing federal interest. The investigation may be continued in such cases with whatever scope is warranted in light of these considerations.
- d. An investigation which has been terminated may be reopened upon a showing of the same standard and pursuant to the same procedures as required for initiation of an investigation.
- e. In addition to the authority of Special Agents in Charge under this paragraph, the Director of the FBI, and any Assistant Director or senior Headquarters official designated by the Director, may authorize, renew, review, and reopen terrorism enterprise investigations in conformity with the standards of this paragraph.
- f. The FBI shall report to the Terrorism and Violent Crime Section of the Criminal Division and the Office of Intelligence Policy and Review the progress of a terrorism enterprise investigation not later than 180 days after its initiation, and the results at the end of each year the investigation continues. The Terrorism and Violent Crime Section shall immediately transmit copies of these reports to the Attorney General and the Deputy Attorney General.

IV. INVESTIGATIVE TECHNIQUES

- A. When conducting investigations under these guidelines, the FBI may use any lawful investigative technique. The choice of investigative techniques is a matter of judgment, which should take account of: (i) the objectives of the investigation and available investigative resources, (ii) the intrusiveness of a technique, considering such factors as the effect on the privacy of individuals and potential damage to reputation, (iii) the seriousness of the crime, and (iv) the strength of the information indicating its existence

or future commission. Where the conduct of an investigation presents a choice between the use of more or less intrusive methods, the FBI should consider whether the information could be obtained in a timely and effective way by the less intrusive means. The FBI should not hesitate to use any lawful techniques consistent with these Guidelines in an investigation, even if intrusive, where the intrusiveness is warranted in light of the seriousness of the crime or the strength of the information indicating its existence or future commission. This point is to be particularly observed in investigations relating to terrorist activities.

- B. All requirements for use of a technique set by statute, Department regulations and policies, or Attorney General Guidelines must be complied with. The investigative techniques listed below are subject to the noted restrictions:
1. Confidential informants must be used in compliance with the Attorney General's Guidelines Regarding the Use of Confidential Informants;
 2. Undercover activities and operations must be conducted in compliance with the Attorney General's Guidelines on FBI Undercover Operations;
 3. In situations involving undisclosed participation in the activities of an organization by an undercover employee or cooperating private individual, any potential constitutional concerns relating to activities of the organization protected by the First Amendment must be addressed through full compliance with all applicable provisions of the Attorney General's Guidelines on FBI Undercover Operations and the Attorney General's Guidelines Regarding the Use of Confidential Informants;
 4. Nonconsensual electronic surveillance must be conducted pursuant to the warrant procedures and requirements of chapter 119 of title 18, United States Code (18 U.S.C. 2510-2522);
 5. Pen registers and trap and trace devices must be installed and used pursuant to the procedures and requirements of chapter 206 of title 18, United States Code (18 U.S.C. 3121-3127);
 6. Access to stored wire and electronic communications and transactional records must be obtained pursuant to the procedures and requirements of chapter 121 of title 18, United States Code (18 U.S.C. 2701-2712);
 7. Consensual electronic monitoring must be authorized pursuant to Department policy. For consensual monitoring of conversations other than telephone conversations, advance authorization must be obtained in accordance with established guidelines. This applies both to devices carried by the cooperating

participant and to devices installed on premises under the control of the participant. See U.S. Attorneys' Manual 9-7.301 and 9-7.302. For consensual monitoring of telephone conversations, advance authorization must be obtained from the SAC or Assistant Special Agent in Charge and the appropriate U.S. Attorney, Assistant Attorney General, or Deputy Assistant Attorney General, except in exigent circumstances. An Assistant Attorney General or Deputy Assistant Attorney General who provides such authorization shall notify the appropriate U.S. Attorney;

8. Searches and seizures must be conducted under the authority of a valid warrant unless the search or seizure comes within a judicially recognized exception to the warrant requirement. See also Attorney General's Guidelines on Methods of Obtaining Documentary Materials Held by Third Parties, 28 CFR Part 59;
9. Classified investigative technologies must be used in compliance with the Procedures for the Use of Classified Investigative Technologies in Criminal Cases; and
10. Whenever an individual is known to be represented by counsel in a particular matter, the FBI shall follow applicable law and Department procedure concerning contact with represented individuals in the absence of prior notice to their counsel. The SAC or his designee and the United States Attorney shall consult periodically on applicable law and Department procedure. Where issues arise concerning the consistency of contacts with represented persons with applicable attorney conduct rules, the United States Attorney should consult with the Professional Responsibility Advisory Office.

V. DISSEMINATION AND MAINTENANCE OF INFORMATION

- A. The FBI may disseminate information during the checking of leads, preliminary inquiries, and investigations conducted pursuant to these Guidelines to United States Attorneys, the Criminal Division, and other components, officials, and officers of the Department of Justice. The FBI may disseminate information during the checking of leads, preliminary inquiries, and investigations conducted pursuant to these Guidelines to another Federal agency or to a State or local criminal justice agency when such information:
 1. falls within the investigative or protective jurisdiction or litigative responsibility of the agency;
 2. may assist in preventing a crime or the use of violence or any other conduct dangerous to human life;

3. is required to be furnished to another Federal agency by Executive Order 10450, as amended, dated April 27, 1953, or a successor Order; or
4. is required to be disseminated by statute, interagency agreement approved by the Attorney General, or Presidential Directive;

and to other persons and agencies as required by 5 U.S.C. 552 or as otherwise permitted by 5 U.S.C. 552a.

- B. The FBI shall maintain a database that identifies all preliminary inquiries and investigations conducted pursuant to these Guidelines and that permits the prompt retrieval of information concerning the status (open or closed) and subjects of all such inquiries and investigations.

VI. COUNTERTERRORISM ACTIVITIES AND OTHER AUTHORIZATIONS

In order to carry out its central mission of preventing the commission of terrorist acts against the United States and its people, the FBI must proactively draw on available sources of information to identify terrorist threats and activities. It cannot be content to wait for leads to come in through the actions of others, but rather must be vigilant in detecting terrorist activities to the full extent permitted by law, with an eye towards early intervention and prevention of acts of terrorism before they occur. This Part accordingly identifies a number of authorized activities which further this end, and which can be carried out even in the absence of a checking of leads, preliminary inquiry, or full investigation as described in Parts I-III of these Guidelines. The authorizations include both activities that are specifically focused on terrorism (Subpart A) and activities that are useful for law enforcement purposes in both terrorism and non-terrorism contexts (Subpart B).

A. COUNTERTERRORISM ACTIVITIES

1. Information Systems

The FBI is authorized to operate and participate in identification, tracking, and information systems for the purpose of identifying and locating terrorists, excluding or removing from the United States alien terrorists and alien supporters of terrorist activity as authorized by law, assessing and responding to terrorist risks and threats, or otherwise detecting, prosecuting, or preventing terrorist activities. Systems within the scope of this paragraph may draw on and retain pertinent information from any source permitted by law, including information derived from past or ongoing investigative activities; other information collected or provided by governmental entities, such as foreign intelligence information and lookout list information; publicly available information, whether obtained directly or through services or resources (whether nonprofit or commercial) that compile

or analyze such information; and information voluntarily provided by private entities. Any such system operated by the FBI shall be reviewed periodically for compliance with all applicable statutory provisions, Department regulations and policies, and Attorney General Guidelines.

2. Visiting Public Places and Events

For the purpose of detecting or preventing terrorist activities, the FBI is authorized to visit any place and attend any event that is open to the public, on the same terms and conditions as members of the public generally. No information obtained from such visits shall be retained unless it relates to potential criminal or terrorist activity.

B. OTHER AUTHORIZATIONS

In addition to the checking of leads, preliminary inquiries, and investigations as described in Parts I-III of these Guidelines, and counterterrorism activities as described in Part A above, the authorized law enforcement activities of the FBI include carrying out and retaining information resulting from the following activities:

1. General Topical Research

The FBI is authorized to carry out general topical research, including conducting online searches and accessing online sites and forums as part of such research on the same terms and conditions as members of the public generally. "General topical research" under this paragraph means research concerning subject areas that are relevant for the purpose of facilitating or supporting the discharge of investigative responsibilities. It does not include online searches for information by individuals' names or other individual identifiers, except where such searches are incidental to topical research, such as searching to locate writings on a topic by searching under the names of authors who write on the topic, or searching by the name of a party to a case in conducting legal research.

2. Use of Online Resources Generally

For the purpose of detecting or preventing terrorism or other criminal activities, the FBI is authorized to conduct online search activity and to access online sites and forums on the same terms and conditions as members of the public generally.

3. Reports and Assessments

The FBI is authorized to prepare general reports and assessments concerning terrorism or other criminal activities for purposes of strategic planning or in support of investigative activities.

4. Cooperation with Secret Service

The FBI is authorized to provide investigative assistance in support of the protective responsibilities of the Secret Service, provided that all preliminary inquiries or investigations are conducted in accordance with the provisions of these Guidelines.

C. PROTECTION OF PRIVACY AND OTHER LIMITATIONS

1. General Limitations

The law enforcement activities authorized by this Part do not include maintaining files on individuals solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of any other rights secured by the Constitution or laws of the United States. Rather, all such law enforcement activities must have a valid law enforcement purpose as described in this Part, and must be carried out in conformity with all applicable statutes, Department regulations and policies, and Attorney General Guidelines. In particular, the provisions of this Part do not supersede any otherwise applicable provision or requirement of the Attorney General's Guidelines on FBI Undercover Operations or the Attorney General's Guidelines Regarding the Use of Confidential Informants.

2. Maintenance of Records Under the Privacy Act

Under the Privacy Act, the permissibility of maintaining records relating to certain activities of individuals depends in part on whether the collection of such information is "pertinent to and within the scope of an authorized law enforcement activity." 5 U.S.C. 552a(e)(7). By its terms, the limitation of 5 U.S.C. 552a(e)(7) is inapplicable to activities that do not involve the "maintain[ing]" of a "record" within the meaning of the Privacy Act, or that occur pertinent to and within the scope of an authorized law enforcement activity. "Authorized law enforcement activit[ies]" for purposes of the Privacy Act include carrying out and retaining information resulting from the checking of leads, preliminary inquiries, or investigations as described in Parts I-III of these Guidelines, or from activities described in Subpart A or B of this Part. As noted in paragraph (3) below, however, this is not an exhaustive enumeration of "authorized law enforcement activit[ies]." Questions about the application of the Privacy Act to other activities should be addressed to the FBI Office of the General Counsel or the Office of Information and Privacy.

3. Construction of Part

This Part does not limit any activities authorized by or carried out under other Parts of these Guidelines. The specification of authorized law enforcement activities under this Part is not exhaustive, and does not limit other authorized law enforcement activities, such as those relating to foreign counterintelligence or foreign intelligence.

VII. RESERVATION

- A. Nothing in these Guidelines shall limit the general reviews or audits of papers, files, contracts, or other records in the government's possession, or the performance of similar services at the specific request of a Department or agency of the United States. Such reviews, audits or similar services must be for the purpose of detecting or preventing violations of federal law which are within the investigative responsibility of the FBI.**
- B. Nothing in these Guidelines is intended to limit the FBI's responsibilities to investigate certain applicants and employees under the federal personnel security program.**
- C. These Guidelines are set forth solely for the purpose of internal Department of Justice guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter, civil or criminal, nor do they place any limitation on otherwise lawful investigative and litigative prerogatives of the Department of Justice.**

Date: May 30, 2002



John Ashcroft
Attorney General