



Office of the Attorney General  
Washington, D. C. 20530

**THE ATTORNEY GENERAL'S GUIDELINES ON  
GENERAL CRIMES, RACKETEERING ENTERPRISE AND  
TERRORISM ENTERPRISE INVESTIGATIONS**

## **PREAMBLE**

As the primary criminal investigative agency in the federal government, the Federal Bureau of Investigation (FBI) has the authority and responsibility to investigate all criminal violations of federal law that are not exclusively assigned to another federal agency. The FBI thus plays a central role in the enforcement of federal laws and in the proper administration of justice in the United States. In discharging this function, the highest priority is to protect the security of the nation and the safety of the American people against the depredations of terrorists and foreign aggressors.

Investigations by the FBI are premised upon the fundamental duty of government to protect the public against general crimes, against organized criminal activity, and against those who would threaten the fabric of our society through terrorism or mass destruction. That duty must be performed with care to protect individual rights and to insure that investigations are confined to matters of legitimate law enforcement interest. The purpose of these Guidelines, therefore, is to establish a consistent policy in such matters. The Guidelines will enable Agents of the FBI to perform their duties with greater certainty, confidence and effectiveness, and will provide the American people with a firm assurance that the FBI is acting properly under the law.

These Guidelines provide guidance for general crimes and criminal intelligence investigations by the FBI. The standards and requirements set forth herein govern the circumstances under which such investigations may be begun, and the permissible scope, duration, subject matters, and objectives of these investigations. They do not limit activities carried out under other Attorney General guidelines addressing such matters as investigations and information collection relating to international terrorism, foreign counterintelligence, or foreign intelligence.

The Introduction that follows explains the background of the reissuance of these Guidelines, their general approach and structure, and their specific application in furtherance of the FBI's central mission to protect the United States and its people from acts of terrorism. Part I sets forth general principles that apply to all investigations conducted under these Guidelines. Part II governs investigations undertaken to prevent, solve or prosecute specific violations of federal law. Subpart A of Part III governs criminal intelligence investigations undertaken to obtain information concerning enterprises which are engaged in racketeering activities. Subpart B of Part III governs criminal intelligence investigations undertaken to obtain information concerning enterprises which seek to further political or social goals through violence or which otherwise aim to engage in terrorism or the commission of terrorism-related crimes. Parts IV through VII discuss authorized investigative techniques, dissemination and maintenance of information, counterterrorism activities and other authorized law enforcement activities, and miscellaneous matters.

These Guidelines are issued under the authority of the Attorney General as provided in sections 509, 510, 533, and 534 of title 28, United States Code.

## **TABLE OF CONTENTS**

<b>INTRODUCTION</b>	<b>1</b>
<b>A.    CHECKING OF LEADS AND PRELIMINARY INQUIRIES .....</b>	<b>1</b>
<b>B.    FULL INVESTIGATIONS .....</b>	<b>2</b>
<b>C.    AUTHORIZED INVESTIGATIVE TECHNIQUES .....</b>	<b>5</b>
<b>D.    OTHER AUTHORIZED ACTIVITIES .</b>	<b>6</b>
<b>I.    <u>GENERAL PRINCIPLES</u></b>	<b>.. 6</b>
<b>II.   <u>GENERAL CRIMES INVESTIGATIONS .</u></b>	<b>7</b>
<b>A.    DEFINITIONS</b>	<b>7</b>
<b>B.    PRELIMINARY INQUIRIES</b>	<b>8</b>
<b>C.    INVESTIGATIONS</b>	
<b>III.  <u>CRIMINAL INTELLIGENCE INVESTIGATIONS</u></b>	<b>12</b>
<b>A.    RACKETEERING ENTERPRISE INVESTIGATIONS</b>	
1.    Definition .	13
2.    General Authority	13
3.    Purpose	14
4.    Scope .....	14
5.    Authorization and Renewal	
<b>B.    TERRORISM ENTERPRISE INVESTIGATIONS</b>	
1.    General Authority	
2.    Purpose . .	16
3.    Scope	17

4.	Authorization and Renewal .....	17
IV.	<b><u>INVESTIGATIVE TECHNIQUES</u></b> .....	18
V.	<b><u>DISSEMINATION AND MAINTENANCE OF INFORMATION</u></b> .....	20
VI.	<b><u>COUNTERTERRORISM ACTIVITIES AND OTHER AUTHORIZATIONS</u></b>	21
A.	<b>COUNTERTERRORISM ACTIVITIES</b> .....	21
	Information Systems ..	21
2.	Visiting Public Places and Events .....	22
B.	<b>OTHER AUTHORIZATIONS</b> ....	22
	General Topical Research .....	22
2.	Use of Online Resources Generally .	22
3	Reports and Assessments .	22
4.	Cooperation with Secret Service ..	23
C.	<b>PROTECTION OF PRIVACY AND OTHER LIMITATIONS</b> .	23
1	General Limitations	23
2.	Maintenance of Records Under the Privacy Act	23
3	Construction of Part	24
VII.	<b><u>RESERVATION</u></b> .	24

## **INTRODUCTION**

Following the September 11, 2001, terrorist attack on the United States, the Department of Justice carried out a general review of existing guidelines and procedures relating to national security and criminal matters. The reissuance of these Guidelines reflects the result of that review.

These Guidelines follow previous guidelines in their classification of levels of investigative activity, in their classification of types of investigations, in their standards for initiating investigative activity, and in their identification of permitted investigative techniques. There are, however, a number of changes designed to enhance the general effectiveness of criminal investigation, to bring the Guidelines into conformity with recent changes in the law, and to facilitate the FBI's central mission of preventing the commission of terrorist acts against the United States and its people.

In their general structure, these Guidelines provide graduated levels of investigative activity, allowing the FBI the necessary flexibility to act well in advance of the commission of planned terrorist acts or other federal crimes. The three levels of investigative activity are: (1) the prompt and extremely limited checking of initial leads, (2) preliminary inquiries, and (3) full investigations. Subject to these Guidelines and other guidelines and policies noted in Part IV below, any lawful investigative technique may be used in full investigations, and with some exceptions, in preliminary inquiries.

### **A. CHECKING OF LEADS AND PRELIMINARY INQUIRIES**

The lowest level of investigative activity is the "prompt and extremely limited checking out of initial leads," which should be undertaken whenever information is received of such a nature that some follow-up as to the possibility of criminal activity is warranted. This limited activity should be conducted with an eye toward promptly determining whether further investigation (either a preliminary inquiry or a full investigation) should be conducted.

The next level of investigative activity, a preliminary inquiry, should be undertaken when there is information or an allegation which indicates the possibility of criminal activity and whose responsible handling requires some further scrutiny beyond checking initial leads. This authority allows FBI agents to respond to information that is ambiguous or incomplete. Even where the available information meets only this threshold, the range of available investigative techniques is broad. These Guidelines categorically prohibit only mail opening and nonconsensual electronic surveillance at this stage. Other methods, including the development of sources and informants and undercover activities and operations, are permitted in preliminary inquiries. The tools available to develop information sufficient for the commencement of a full investigation, or determining that one is not merited – the purpose of a preliminary inquiry – should be fully employed, consistent with these Guidelines, with a view toward preventing terrorist activities.

Whether it is appropriate to open a preliminary inquiry immediately, or instead to engage first in a limited checking out of leads, depends on the circumstances presented. If, for example, an agent receives an allegation that an individual or group has advocated the commission of criminal violence, and no other facts are available, an appropriate first step would be checking out of leads to determine whether the individual, group, or members of the audience have the apparent ability or intent to carry out the advocated crime. A similar response would be appropriate on the basis of non-verbal conduct of an ambiguous character – for example, where a report is received that an individual has accumulated explosives that could be used either in a legitimate business or to commit a terrorist act. Where the limited checking out of leads discloses a possibility or reasonable indication of criminal activity, a preliminary inquiry or full investigation may then be initiated. However, if the available information shows at the outset that the threshold standard for a preliminary inquiry or full investigation is satisfied, then the appropriate investigative activity may be initiated immediately, without progressing through more limited investigative stages.

The application of these Guidelines' standards for inquiries merits special attention in cases that involve efforts by individuals or groups to obtain, for no apparent reason, biological, chemical, radiological, or nuclear materials whose use or possession is constrained by such statutes as 18 U.S.C. 175, 229, or 831. For example, FBI agents are not required to possess information relating to an individual's intended criminal use of dangerous biological agents or toxins prior to initiating investigative activity. On the contrary, if an individual or group has attempted to obtain such materials, or has indicated a desire to acquire them, and the reason is not apparent, investigative action, such as conducting a checking out of leads or initiating a preliminary inquiry, may be appropriate to determine whether there is a legitimate purpose for the possession of the materials by the individual or group. Likewise, where individuals or groups engage in efforts to acquire or show an interest in acquiring, without apparent reason, toxic chemicals or their precursors or radiological or nuclear materials, investigative action to determine whether there is a legitimate purpose may be justified.

## **B. FULL INVESTIGATIONS**

These Guidelines provide for two types of full investigations: general crimes investigations (Part II below) and criminal intelligence investigations (Part III below). The choice of the type of investigation depends on the information and the investigative focus. A general crimes investigation may be initiated where facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed. Preventing future criminal activity, as well as solving and prosecuting crimes that have already occurred, is an explicitly authorized objective of general crimes investigations. The "reasonable indication" threshold for undertaking such an investigation is substantially lower than probable cause. In addition, preparation to commit a criminal act can itself 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). Under these Guidelines, a general crimes

investigation is warranted where there is not yet a current substantive or preparatory crime, but where facts or circumstances reasonably indicate that such a crime will occur in the future.

The second type of full investigation authorized under these Guidelines is the criminal intelligence investigation. The focus of criminal intelligence investigations is the group or enterprise, rather than just individual participants and specific acts. The immediate purpose of such an investigation is to obtain information concerning the nature and structure of the enterprise – including information relating to the group’s membership, finances, geographical dimensions, past and future activities, and goals – with a view toward detecting, preventing, and prosecuting the enterprise’s criminal activities. Criminal intelligence investigations, usually of a long-term nature, may provide vital intelligence to help prevent terrorist acts.

Authorized criminal intelligence investigations are of two types: racketeering enterprise investigations (Part III.A) and terrorism enterprise investigations (Part III.B).

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 Racketeer Influenced and Corrupt Organizations Act (RICO). However, the USA PATRIOT ACT (Public Law 107-56) expanded the predicate acts for RICO to include the crimes most likely to be committed by terrorists and their supporters, as described in 18 U.S.C. 2332b(g)(5)(B). To maintain uniformity in the standards and procedures for criminal intelligence investigations relating to terrorism, investigations premised on racketeering activity involving offenses described in 18 U.S.C. 2332b(g)(5)(B) are subject to the provisions for terrorism enterprise investigations rather than those for racketeering enterprise investigations.

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: (1) furthering political or social goals wholly or in part through activities that involve force or violence and a federal crime, (2) engaging in terrorism as defined in 18 U.S.C. 2331(1) or (5) that involves a federal crime, or (3) committing any offense described in 18 U.S.C. 2332b(g)(5)(B). As noted above, criminal intelligence investigations premised on a pattern of racketeering activity involving an 18 U.S.C. 2332b(g)(5)(B) offense are also treated as terrorism enterprise investigations.

As with the other types of full investigations authorized by these Guidelines, any lawful investigative technique may be used in terrorism enterprise investigations, including the development of sources and informants and undercover activities and operations. The “reasonable indication” standard for commencing a terrorism enterprise investigation is the same as that for general crimes and racketeering enterprise investigations. As noted above, it is substantially lower than probable cause.

In practical terms, the “reasonable indication” standard for opening a criminal intelligence investigation of an enterprise in the terrorism context could be satisfied in a number of ways. In

some cases satisfaction of the standard will be apparent on the basis of direct evidence of an enterprise's involvement in or planning for the commission of a federal offense involving the use of force or violence to further political or social goals, terrorism as defined in 18 U.S.C. 2331(1) or (5), or a crime described in 18 U.S.C. 2332b(g)(5)(B). For example, direct information may be available about statements made in furtherance of an enterprise's objectives which show a purpose of committing such crimes or securing their commission by others.

In other cases, the nature of the conduct engaged in by an enterprise will justify an inference that the standard is satisfied, even if there are no known statements by participants that advocate or indicate planning for violence or other prohibited acts. For example, such activities as attempting to obtain dangerous biological agents, toxic chemicals, or nuclear materials, or stockpiling explosives or weapons, with no discernible lawful purpose, may be sufficient to reasonably indicate that an enterprise aims to engage in terrorism.

Moreover, a group's activities and the statements of its members may properly be considered in conjunction with each other. A combination of statements and activities may justify a determination that the threshold standard for a terrorism enterprise investigation is satisfied, even if the statements alone or the activities alone would not warrant such a determination.

While no particular factor or combination of factors is required, considerations that will generally be relevant to the determination whether the threshold standard for a terrorism enterprise investigation is satisfied include, as noted, a group's statements, its activities, and the nature of potential federal criminal law violations suggested by its statements or activities. Thus, where there are grounds for inquiry concerning a group, it may be helpful to gather information about these matters, and then to consider whether these factors, either individually or in combination, reasonably indicate that the group is pursuing terrorist activities or objectives as defined in the threshold standard. Findings that would weigh in favor of such a conclusion include, for example, the following:

**(1) Threats or advocacy of violence or other covered criminal acts:**

Statements are made in relation to or in furtherance of an enterprise's political or social objectives that threaten or advocate the use of force or violence, or statements are made in furtherance of an enterprise that otherwise threaten or advocate criminal conduct within the scope of 18 U.S.C. 2331(1) or (5) or 2332b(g)(5)(B), which may concern such matters as (e.g.):

- (i) engaging in attacks involving or threatening massive loss of life or injury, mass destruction, or endangerment of the national security;
- (ii) killing or injuring federal personnel, destroying federal facilities, or defying lawful federal authority;



(iii) killing, injuring or intimidating individuals because of their status as United States nationals or persons, or because of their national origin, race, color, religion, or sex; or

(iv) depriving individuals of any rights secured by the Constitution or laws of the United States.

**(2) Apparent ability or intent to carry out violence or other covered activities:**

The enterprise manifests an apparent ability or intent to carry out violence or other activities within the scope of 18 U.S.C. 2331(1) or (5) or 2332b(g)(5)(B), e.g.:

(i) by acquiring, or taking steps towards acquiring, biological agents or toxins, toxic chemicals or their precursors, radiological or nuclear materials, explosives, or other destructive or dangerous materials (or plans or formulas for such materials), or weapons, under circumstances where, by reason of the quantity or character of the items, the lawful purpose of the acquisition is not apparent;

(ii) by the creation, maintenance, or support of an armed paramilitary organization;

(iii) by paramilitary training; or

(iv) by other conduct demonstrating an apparent ability or intent to injure or intimidate individuals, or to interfere with the exercise of their constitutional or statutory rights.

**(3) Potential federal crime:**

The group's statements or activities suggest potential federal criminal violations that may be relevant in applying the standard for initiating a terrorism enterprise investigation – such as crimes under the provisions of the U.S. Code that set forth specially defined terrorism or support-of-terrorism offenses, or that relate to such matters as aircraft hijacking or destruction, attacks on transportation, communications, or energy facilities or systems, biological or chemical weapons, nuclear or radiological materials, civil rights violations, assassinations or other violence against federal officials or facilities, or explosives (e.g., the offenses listed in 18 U.S.C. 2332b(g)(5)(B) or appearing in such provisions as 18 U.S.C. 111, 115, 231, 241, 245, or 247).

## **C. AUTHORIZED INVESTIGATIVE TECHNIQUES**

All lawful investigative techniques may be used in general crimes, racketeering enterprise, and terrorism enterprise investigations. In preliminary inquiries, these Guidelines bar the use of mail openings and nonconsensual electronic surveillance (including all techniques covered by chapter 119 of title 18, United States Code), but do not categorically prohibit the use

of any other lawful investigative technique at that stage. As set forth in Part IV below, authorized methods in investigations include, among others, use of confidential informants, undercover activities and operations, nonconsensual electronic surveillance, pen registers and trap and trace devices, accessing stored wire and electronic communications and transactional records, consensual electronic monitoring, and searches and seizures. All requirements for the use of such methods under the Constitution, applicable statutes, and Department regulations or policies must, of course, be observed.

#### **D. OTHER AUTHORIZED ACTIVITIES**

Current counterterrorism priorities and the advent of the Internet have raised a number of issues which did not exist in any comparable form when the last general revision of these Guidelines was carried out in 1989 – a time long preceding the September 11 attack’s disclosure of the full magnitude of the terrorist threat to the United States, and a time in which the Internet was not available in any developed form as a source of information for counterterrorism and other anti-crime purposes. Part VI of these Guidelines is designed to provide clear authorizations and statements of governing principles for a number of important activities that affect these areas. Among other things, Part VI makes it clear that the authorized law enforcement activities of the FBI include: (i) operating and participating in counterterrorism information systems, such as the Foreign Terrorist Tracking Task Force (VI.A(1)); (ii) visiting places and events which are open to the public for the purpose or detecting or preventing terrorist activities (VI.A(2)); (iii) carrying out general topical research, such as searching online under terms like “anthrax” or “smallpox” to obtain publicly available information about agents that may be used in bioterrorism attacks (VI.B(1)); (iv) surfing the Internet as any member of the public might do to identify, *e.g.*, public websites, bulletin boards, and chat rooms in which bomb making instructions, child pornography, or stolen credit card information is openly traded or disseminated, and observing information open to public view in such forums to detect terrorist activities and other criminal activities (VI.B(2)); (v) preparing general reports and assessments relating to terrorism or other criminal activities in support of strategic planning and investigative operations (VI.B(3)); and (vi) providing investigative assistance to the Secret Service in support of its protective responsibilities (VI.B(4)).

#### **I. GENERAL PRINCIPLES**

Preliminary inquiries and investigations governed by these Guidelines are conducted for the purpose of preventing, detecting, or prosecuting violations of federal law. The FBI shall fully utilize the methods authorized by these Guidelines to maximize the realization of these objectives.

The conduct of preliminary inquiries and investigations may present choices between the use of investigative methods which are more or less intrusive, considering such factors as the effect on the privacy of individuals and potential damage to reputation. Inquiries and investigations shall be conducted with as little intrusion as the needs of the situation permit. It is

recognized, however, that the choice of techniques is a matter of judgment. The FBI shall not hesitate to use any lawful techniques consistent with these Guidelines, even if intrusive, where the intrusiveness is warranted in light of the seriousness of a crime or the strength of the information indicating its commission or potential future commission. This point is to be particularly observed in the investigation of terrorist crimes and in the investigation of enterprises that engage in terrorism.

All preliminary inquiries shall be conducted pursuant to the General Crimes Guidelines (i.e., Part II of these Guidelines). There is no separate provision for preliminary inquiries under the Criminal Intelligence Guidelines (i.e., Part III of these Guidelines) because preliminary inquiries under Part II may be carried out not only to determine whether the grounds exist to commence a general crimes investigation under Part II, but alternatively or in addition to determine whether the grounds exist to commence a racketeering enterprise investigation or terrorism enterprise investigation under Part III. A preliminary inquiry shall be promptly terminated when it becomes apparent that a full investigation is not warranted. If, on the basis of information discovered in the course of a preliminary inquiry, an investigation is warranted, it may be conducted as a general crimes investigation, or a criminal intelligence investigation, or both. All such investigations, however, shall be based on a reasonable factual predicate and shall have a valid law enforcement purpose.

In its efforts to anticipate or prevent crime, the FBI must at times initiate investigations in advance of criminal conduct. It is important that such investigations not be based solely on activities protected by the First Amendment or on the lawful exercise of any other rights secured by the Constitution or laws of the United States. When, however, statements advocate criminal activity or indicate an apparent intent to engage in crime, particularly crimes of violence, an investigation under these Guidelines may be warranted unless it is apparent, from the circumstances or the context in which the statements are made, that there is no prospect of harm.

General crimes investigations and criminal intelligence investigations shall be terminated when all logical leads have been exhausted and no legitimate law enforcement interest justifies their continuance.

Nothing in these Guidelines prohibits the FBI from ascertaining the general scope and nature of criminal activity in a particular location or sector of the economy, or from collecting and maintaining publicly available information consistent with the Privacy Act.

## **II. GENERAL CRIMES INVESTIGATIONS**

### **A. DEFINITIONS**

(1) "Exigent circumstances" are circumstances requiring action before authorization otherwise necessary under these guidelines can reasonably be obtained, in order to protect life or substantial property interests; to apprehend or identify a fleeing

offender; to prevent the hiding, destruction or alteration of evidence; or to avoid other serious impairment or hindrance of an investigation.

(2) "Sensitive criminal matter" is any alleged criminal conduct involving corrupt action by a public official or political candidate, the activities of a foreign government, the activities of a religious organization or a primarily political organization or the related activities of any individual prominent in such an organization, or the activities of the news media; and any other matter which in the judgment of a Special Agent in Charge (SAC) should be brought to the attention of the United States Attorney or other appropriate official in the Department of Justice, as well as FBI Headquarters (FBIHQ).

## **B. PRELIMINARY INQUIRIES**

(1) On some occasions the FBI may receive information or an allegation not warranting a full investigation – because there is not yet a "reasonable indication" of criminal activities – but whose responsible handling requires some further scrutiny beyond the prompt and extremely limited checking out of initial leads. In such circumstances, though the factual predicate for an investigation has not been met, the FBI may initiate an "inquiry" in response to the allegation or information indicating the possibility of criminal activity.

This authority to conduct inquiries short of a full investigation allows the government to respond in a measured way to ambiguous or incomplete information, with as little intrusion as the needs of the situation permit. This is especially important in such areas as white-collar crime where no complainant is involved or when an allegation or information is received from a source of unknown reliability. Such inquiries are subject to the limitations on duration under paragraph (3) below and are carried out to obtain the information necessary to make an informed judgment as to whether a full investigation is warranted.

A preliminary inquiry is not a required step when facts or circumstances reasonably indicating criminal activity are already available; in such cases, a full investigation can be immediately opened.

(2) The FBI supervisor authorizing an inquiry shall assure that the allegation or other information which warranted the inquiry has been recorded in writing. In sensitive criminal matters, the United States Attorney or an appropriate Department of Justice official shall be notified of the basis for an inquiry as soon as practicable after the opening of the inquiry, and the fact of notification shall be recorded in writing.

(3) Inquiries shall be completed within 180 days after initiation of the first investigative step. The date of the first investigative step is not necessarily the same date on which the first incoming information or allegation was received. An extension of time

in an inquiry for succeeding 90-day periods may be granted. A SAC may grant up to two extensions based on a statement of the reasons why further investigative steps are warranted when there is no "reasonable indication" of criminal activity. All extensions following the second extension may only be granted by FBI Headquarters upon receipt of a written request and such a statement of reasons.

(4) The choice of investigative techniques in an inquiry is a matter of judgment, which should take account of: (i) the objectives of the inquiry 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 possible crime, and (iv) the strength of the information indicating its existence or future commission. Where the conduct of an inquiry 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 inquiry, even if intrusive, where the intrusiveness is warranted in light of the seriousness of the possible crime or the strength of the information indicating its existence or future commission. This point is to be particularly observed in inquiries relating to possible terrorist activities.

(5) All lawful investigative techniques may be used in an inquiry except:

- (a) Mail openings; and
- (b) Nonconsensual electronic surveillance or any other investigative technique covered by chapter 119 of title 18, United States Code (18 U.S.C. 2510-2522).

(6) The following investigative techniques may be used in an inquiry without any prior authorization from a supervisory agent:

- (a) Examination of FBI indices and files;
- (b) Examination of records available to the public and other public sources of information;
- (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;
  - the finances of the enterprise;
  - the geographical dimensions of the enterprise; and
  - 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;  
  
the geographical dimensions of the enterprise; and  
  
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:

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:

---

John Ashcroft  
Attorney General