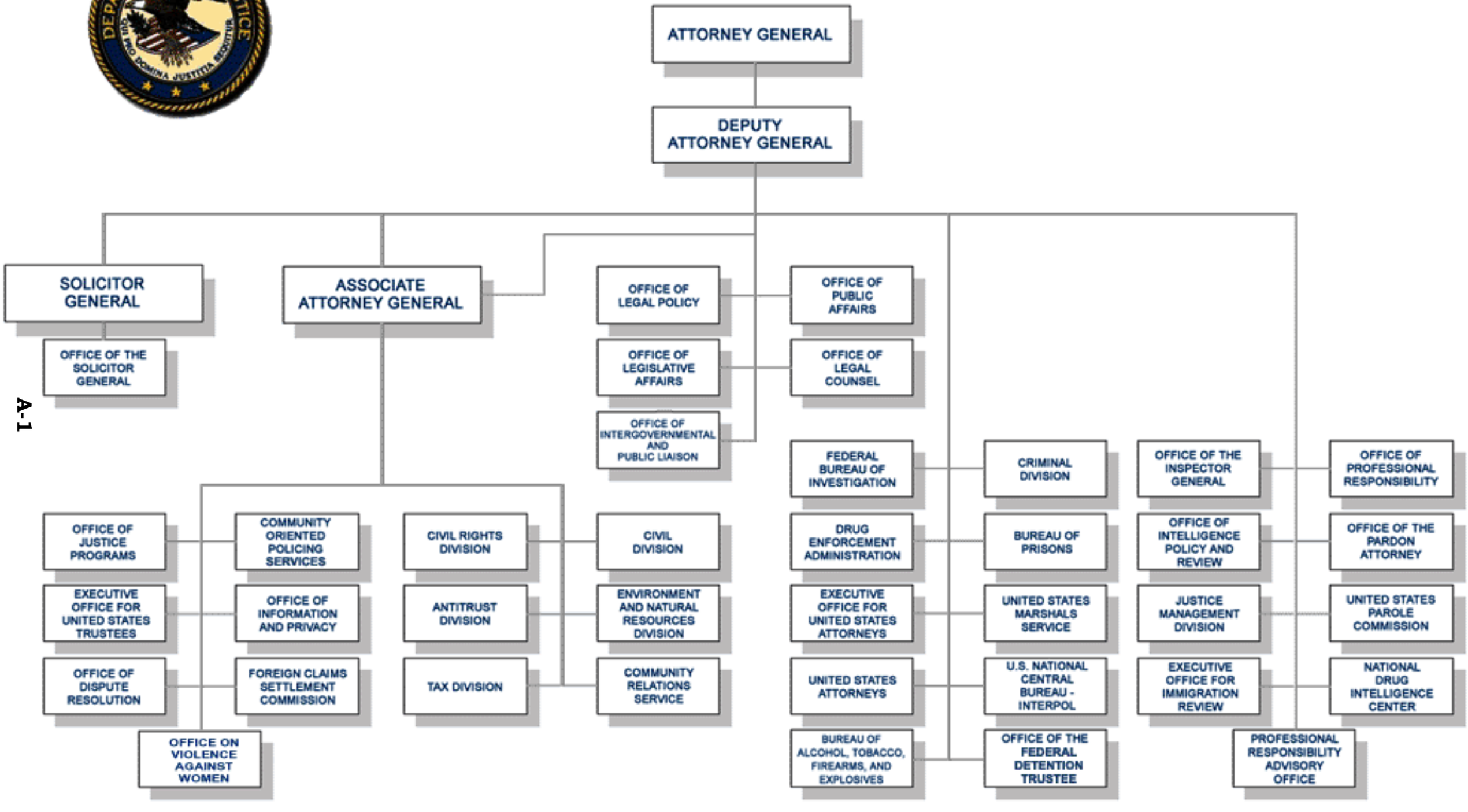
# APPENDIX A

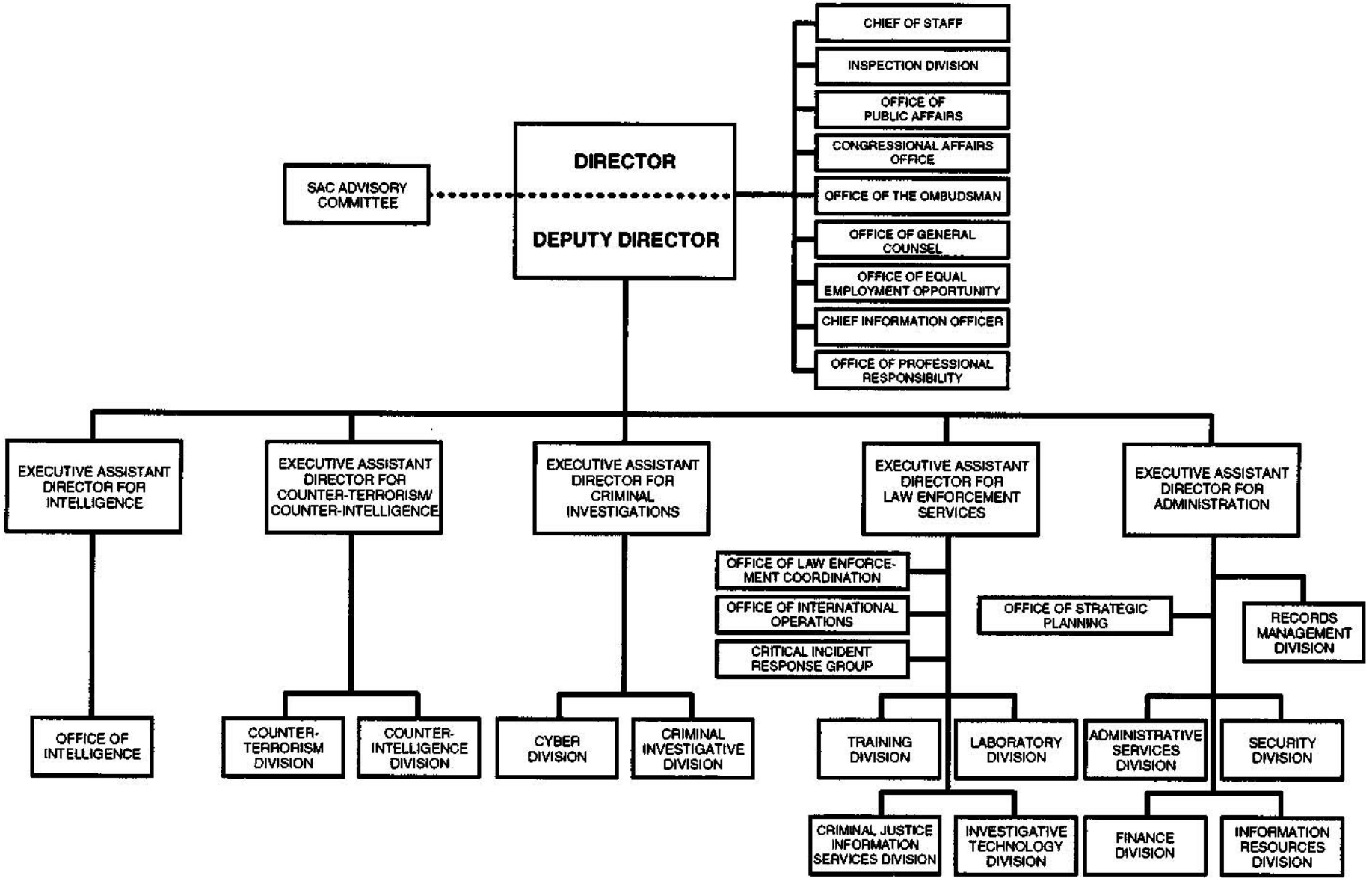
# DEPARTMENT OF JUSTICE




Approved by: _____ Date: 7-14-03

JOHN D. ASHCROFT
Attorney General

# FEDERAL BUREAU OF INVESTIGATION






Approved by: _____ Date: 3-04-04

JOHN ASHCROFT

# APPENDIX B

# THE ATTORNEY GENERAL'S GUIDELINES REGARDING THE USE OF CONFIDENTIAL INFORMANTS

## Preamble

The following Guidelines regarding the use of confidential informants are issued under the authority of the Attorney General as provided in sections 509, 510, and 533 of title 28, United States Code. They apply to the use of confidential informants in criminal investigations and prosecutions by Department of Justice law enforcement agencies and federal prosecuting offices as specified in paragraph (I)(A) below.

## TABLE OF CONTENTS

## I. GENERAL PROVISIONS

### A. PURPOSE AND SCOPE

1. The purpose of these Guidelines is to set policy regarding the use of Confidential Informants, as defined below, in criminal investigations and prosecutions by all Department of Justice Law Enforcement Agencies and Federal Prosecuting Offices, as defined below.

2. These Guidelines do not apply to the use of Cooperating Defendants/Witnesses or Sources of Information, as defined below, unless a Department of Justice Law Enforcement Agency, in its discretion, chooses to apply these Guidelines to such persons.

3. These Guidelines are mandatory and supersede the Attorney General's Guidelines on the Use of Informants in Domestic Security, Organized Crime, and Other Criminal Investigations (December 15, 1976); the Attorney General's Guidelines on FBI Use of Informants and Confidential Sources (December 2, 1980); Resolution 18 of the Office of Investigative Agency Policies (August 15, 1996); and any other guidelines or policies that are inconsistent with these Guidelines. These Guidelines do not supersede otherwise applicable ethical obligations of Department of Justice attorneys, which can, in certain circumstances (for example, with respect to contacts with represented persons), have an impact on law enforcement agents' conduct.

4. These Guidelines do not limit the ability of a Department of Justice Law Enforcement Agency to impose additional restrictions on the use of Confidential Informants.

5. These Guidelines apply to the use of a Confidential Informant in a foreign country only to the extent that the Confidential Informant is reasonably likely to be called to testify in a domestic case.

6. These Guidelines do not apply to the use of Confidential Informants in foreign intelligence or foreign counterintelligence investigations.

### B. DEFINITIONS

1. "Department of Justice Law Enforcement Agency" or "JLEA" –

   a. The Drug Enforcement Administration;

   b. The Federal Bureau of Investigation;

   c. The Immigration and Naturalization Service;

d. The United States Marshals Service; and

e. The Department of Justice Office of the Inspector General.

2. "Field Manager" – a JLEA's first-line supervisor, as defined by the JLEA (typically, GS-14 rank or higher).

3. "Senior Field Manager" – a JLEA's second-line supervisor, as defined by the JLEA (typically, GS-15 rank or higher).

4. "Federal Prosecuting Office" or "FPO" –

a. The United States Attorneys' Offices;

b. The Criminal Division, Tax Division, Civil Rights Division, Antitrust Division, and Environmental and Natural Resources Division of the Department of Justice; and

c. Any other litigating component of the Department of Justice with authority to prosecute federal criminal offenses.

5. "Chief Federal Prosecutor" – the head of a FPO.

6. "Confidential Informant" or "CI" – any individual who provides useful and credible information to a JLEA regarding felonious criminal activities, and from whom the JLEA expects or intends to obtain additional useful and credible information regarding such activities in the future.

7. "Cooperating Defendant/Witness" – any individual who:

a. meets the definition of a CI;

b. has agreed to testify in a proceeding as a result of having provided information to the JLEA; and

c. (i) is a defendant or potential witness who has a written agreement with a FPO, pursuant to which the individual has an expectation of future judicial or prosecutive consideration or assistance as a result of having provided information to the JLEA, or

(ii) is a potential witness who has had a FPO concur in all material aspects of his or her use by the JLEA.

8. "Source of Information" – any individual who:

   a. meets the definition of a CI;

   b. provides information to a JLEA solely as a result of legitimate routine access to information or records, such as an employee of the military, a law enforcement agency, or a legitimate business (e.g., phone company, banks, airlines), and not as a result of criminal association with persons of investigative interest to the JLEA; and

   c. provides such information in a manner consistent with applicable law.

9. "High Level Confidential Informant" – a CI who is part of the senior leadership of an enterprise that

   a. has: (i) a national or international sphere of activities, or (ii) high significance to the JLEA's national objectives, even if the enterprise's sphere of activities is local or regional; and

   b. engages in, or uses others to commit, any of the conduct described below in paragraph (I)(B)(10)(b)(i)-(iv).

10. "Tier 1 Otherwise Illegal Activity" – any activity that:

   a. would constitute a misdemeanor or felony under federal, state, or local law if engaged in by a person acting without authorization; and

   b. that involves –

      (i) the commission, or the significant risk of the commission, of any act of violence by a person or persons other than the Confidential Informant;[1]

      (ii) corrupt conduct, or the significant risk of corrupt conduct, by senior federal, state, or local public officials;

---

[1] Bookmaking that is significantly associated with, or substantially controlled by, organized crime ordinarily will be within the scope of paragraph (I)(B)(10)(b)(i). Thus, for example, where bookmakers have a financial relationship with members or associates of organized crime, and/or use members or associates of organized crime to collect their debts, the conduct of those bookmakers would create a significant risk of violence, and would therefore fall within the definition of Tier 1 Otherwise Illegal Activity.

(iii) the manufacturing, importing, exporting, possession, or trafficking of controlled substances in a quantity equal to or exceeding those quantities specified in United States Sentencing Guidelines § 2D1.1(c)(1);

(iv) financial loss, or the significant risk of financial loss, in an amount equal to or exceeding those amounts specified in United States Sentencing Guidelines § 2B1.1(b)(1)(I);[2]

(v) a Confidential Informant providing to any person (other than a JLEA agent) any item, service, or expertise that is necessary for the commission of a federal, state, or local offense, which the person otherwise would have difficulty obtaining; or

(vi) a Confidential Informant providing to any person (other than a JLEA agent) any quantity of a controlled substance, with little or no expectation of its recovery by the JLEA.

11. "Tier 2 Otherwise Illegal Activity" – any other activity that would constitute a misdemeanor or felony under federal, state, or local law if engaged in by a person acting without authorization.

12. "Fugitive" – an individual:

a. for whom a federal, state, or local law enforcement agency has placed a wanted record in the NCIC (other than for a traffic or petty offense);

b. who is located either within the United States or in a country with which the United States has an extradition treaty; and

---

[2] The citations to the United States Sentencing Guidelines (USSG) Manual are to the 2001 Edition. The references herein to particular USSG Sections are intended to remain applicable to the most closely corresponding USSG level in subsequent editions of the USSG Manual in the event that the cited USSG provisions are amended. Thus, it is intended that subsection (iii) of this paragraph will remain applicable to the highest offense level in the Drug Quantity Table in future editions of the USSG Manual, and that subsection (iv) of the paragraph will remain applicable to dollar amounts that, in future editions of the USSG Manual, trigger sentencing enhancements similar to that set forth in the current section 2B1.1(b)(1)(I). Any ambiguities in this regard should be resolved by the Assistant Attorney General for the Criminal Division.

c. whom the law enforcement agency that has placed the wanted record in the NCIC is willing to take into custody upon his or her arrest and, if necessary, seek his or her extradition to its jurisdiction.

13. "Confidential Informant Review Committee" or "CIRC" – a committee, created by a JLEA for purposes of reviewing certain decisions relating to the registration and utilization of CIs, the chair of which is a JLEA official at or above the level of Deputy Assistant Director (or its equivalent) and the membership of which includes the following two representatives designated by the Assistant Attorney General for the Criminal Division of the Department of Justice (each of whom shall be considered a "Criminal Division representative"): (i) a Deputy Assistant Attorney General for the Criminal Division; and (ii) an Assistant United States Attorney.

## C. PROHIBITION ON COMMITMENTS OF IMMUNITY BY FEDERAL LAW ENFORCEMENT AGENCIES

A JLEA agent does not have any authority to make any promise or commitment that would prevent the government from prosecuting an individual for criminal activity that is not authorized pursuant to paragraph (III)(C) below, or that would limit the use of any evidence by the government, without the prior written approval of the FPO that has primary jurisdiction to prosecute the CI for such criminal activity. A JLEA agent must take the utmost care to avoid giving any person the erroneous impression that he or she has any such authority.

## D. REVEALING A CONFIDENTIAL INFORMANT'S TRUE IDENTITY

Except in the case of approvals and reviews described below in paragraphs (II)(A)(3) (review of long-term CIs), (III)(B)(8) (coordination concerning payments to CIs), (IV)(D)(1) (notification that CI has obtained privileged information), and (V)(D) (coordination concerning deactivation of CI, but only with respect to a CI whose identity was not previously disclosed), whenever a JLEA is required to make contact of any kind with a FPO pursuant to these Guidelines regarding a CI, the JLEA may not withhold the true identity of the CI from the FPO.

## E. DUTY OF CANDOR

Employees of the entities to which these Guidelines apply have a duty of candor in the discharge of their responsibilities pursuant to these Guidelines.

## F. MAINTAINING CONFIDENTIALITY

1. A JLEA agent must take the utmost care to avoid conveying any confidential investigative information to a CI (e.g., information relating to electronic

surveillance, search warrants, or the identity of other actual or potential informants), other than what is necessary and appropriate for operational reasons.

2. The Chief Federal Prosecutor and his or her designee are required to maintain as confidential the identity of any CI and the information the CI has provided, unless obligated to disclose it by law or Court order. If a JLEA provides the Chief Federal Prosecutor or his or her designee with written material containing such information:

   a. Such individual is obligated to keep it confidential by placing it into a locked file cabinet when not in his or her direct care and custody;

   b. Access to the information shall be restricted to the Chief Federal Prosecutor or his or her designee and personnel deemed necessary to carry out the official duties related to the case;

   c. The Chief Federal Prosecutor or his or her designee is responsible for assuring that each person permitted access to the information is made aware of the need to preserve the security and confidentiality of the information, as provided in this policy;

   d. Prior to disclosure of the information to defense counsel or in open Court, the Chief Federal Prosecutor or his or her designee must give the JLEA an opportunity to discuss such disclosure and must comply with any other applicable provision of 28 C.F.R. §§ 16.21-16.29; and

   e. At the conclusion of a case or investigation, all written materials containing the information that have not been disclosed shall be forwarded to the JLEA that provided them.[3]

3. Employees of a JLEA and employees of a FPO have a continuing obligation after leaving employment with the Department of Justice and its constituent components to maintain as confidential the identity of any CI and the information he or she provided, unless the employee is obligated to disclose it by law or Court order. See 28 C.F.R. §§ 16.21 - 16.29.

---

[3] This requirement shall not prevent the Chief Federal Prosecutor or his or her designee from keeping in the relevant case file materials such as motions, responses, legal memoranda, Court orders, and internal office memoranda and correspondence. If any such materials contain information revealing a CI's true identity, the Chief Federal Prosecutor or his or her designee shall maintain the materials in accordance with the provisions of paragraph I(F)(2)(a)-(d), above.

## G. EXCEPTIONS AND DISPUTE RESOLUTION

1. Whenever any of the entities to which these Guidelines apply believes that an exception to any provision of these Guidelines is justified, or whenever there is a dispute between or among any such entities (other than a dispute with the Criminal Division of the Department of Justice) regarding these Guidelines, an exception must be sought from, or the dispute shall be resolved by, the Assistant Attorney General (AAG) for the Criminal Division or his or her designee. The Deputy Attorney General or his or her designee shall hear appeals, if any, from decisions of the AAG.

2. Whenever there is a dispute between the Criminal Division and any of the other entities to which these Guidelines apply, such dispute shall be resolved by the Deputy Attorney General or his or her designee.

3. Any exception granted or dispute resolved pursuant to this paragraph shall be documented in the JLEA's files.

## H. RIGHTS OF THIRD PARTIES

Nothing in these Guidelines is intended to create or does create an enforceable legal right or private right of action by a CI or any other person.

## I. COMPLIANCE

1. Within 120 days of the approval of these Guidelines by the Attorney General, each JLEA shall develop agency-specific guidelines that comply with these Guidelines, and submit such agency-specific guidelines to the AAG for the Criminal Division for review. The agency-specific guidelines must ensure, at a minimum, that the JLEA's agents receive sufficient initial and in-service training in the use of CIs consistent with these Guidelines, and that compliance with these Guidelines is considered in the annual performance appraisal of its agents. As part of such compliance the JLEA shall designate a senior official to oversee all aspects of its CI program, including the training of agents; registration, review and termination of CIs; and notifications to outside entities.

2. Within 30 days of the approval of these Guidelines, each JLEA shall establish a Confidential Informant Review Committee (CIRC) for the purpose of conducting the review procedures specified in paragraphs (II)(A)(3), (II)(D)(1), and (II)(D)(2).

## II. REGISTERING A CONFIDENTIAL INFORMANT

### A. SUITABILITY DETERMINATION

#### 1. Initial Suitability Determination

Prior to utilizing a person as a CI, a case agent of a JLEA shall complete and sign a written Initial Suitability Report and Recommendation, which shall be forwarded to a Field Manager for his or her written approval. In completing the Initial Suitability Report and Recommendation, the case agent must address the following factors (or indicate that a particular factor is not applicable):

a. the person's age;

b. the person's alien status;

c. whether the person is a public official, law enforcement officer, union official, employee of a financial institution or school, member of the military services, a representative or affiliate of the media, or a party to, or in a position to be a party to, privileged communications (e.g., a member of the clergy, a physician, or a lawyer);

d. the extent to which the person would make use of his or her affiliations with legitimate organizations in order to provide information or assistance to the JLEA, and the ability of the JLEA to ensure that the person's information or assistance is limited to criminal matters;

e. the extent to which the person's information or assistance would be relevant to a present or potential investigation or prosecution and the importance of such investigation or prosecution;

f. the nature of any relationship between the CI and the subject or target of an existing or potential investigation or prosecution, including but not limited to a current or former spousal relationship or other family tie, and any current or former employment or financial relationship;

g. the person's motivation in providing information or assistance, including any consideration sought from the government for this assistance;

h. the risk that the person might adversely affect a present or potential investigation or prosecution;

i. the extent to which the person's information or assistance can be corroborated;

j. the person's reliability and truthfulness;

k. the person's prior record as a witness in any proceeding;

l. whether the person has a criminal history, is reasonably believed to be the subject or target of a pending criminal investigation, is under arrest, or has been charged in a pending prosecution;

m. whether the person is reasonably believed to pose a danger to the public or other criminal threat, or is reasonably believed to pose a risk of flight;

n. whether the person is a substance abuser or has a history of substance abuse;

o. whether the person is a relative of an employee of any law enforcement agency;

p. the risk of physical harm that may occur to the person or his or her immediate family or close associates as a result of providing information or assistance to the JLEA; and

q. the record of the JLEA and the record of any other law enforcement agency (if available to the JLEA) regarding the person's prior or current service as a CI, Cooperating Defendant/Witness, or Source of Information, including, but not limited to, any information regarding whether the person was at any time terminated for cause.

2. **Continuing Suitability Review**

a. Each CI's file shall be reviewed by the case agent at least annually. The case agent shall complete and sign a written Continuing Suitability Report and Recommendation, which shall be forwarded to a Field Manager for his or her written approval. In completing the Continuing Suitability Report and Recommendation, the case agent must address the factors set forth above in paragraph (II)(A)(1) (or indicate that a particular factor is not applicable) and, in addition, the length of time that the individual has been registered as a CI and the length of time that the individual has been handled by the same agent or agents.

b. Each JLEA shall establish systems to ensure that all available information that might materially alter a prior suitability determination, including, but not limited to, information pertaining to unauthorized illegal activity by the CI, is promptly reported to a Field Manager and then recorded and maintained in the CI's file. See (IV)(B)(2) below. Upon receipt of any such information, the Field Manager shall ensure that a new Continuing Suitability Report and Recommendation is promptly prepared in light of such new information.

**3. Review of Long-Term Confidential Informants[4]**

a. When a CI has been registered for more than six consecutive years, and, to the extent such a CI remains open, every six years thereafter, the CIRC shall review the CI's completed Initial and Continuing Suitability Reports and Recommendations and decide whether, and under what conditions, the individual should continue to be utilized as a CI. A Criminal Division representative on the CIRC who disagrees with the decision to approve the continued use of such an individual as a Confidential Informant may seek review of that decision pursuant to paragraph (I)(G).

b. Every three years after a CI's file is reviewed pursuant to the provisions of paragraph (II)(A)(3)(a), if the CI remains registered, the JLEA shall conduct an internal review, including review by a designated senior headquarters official, of the CI's completed Initial and Continuing Suitability Reports and Recommendations. If the designated senior headquarters official decides that there are any apparent or potential problems that may warrant any change in the use of the CI, the official shall (i) consult the appropriate Senior Field Manager and (ii) provide the Initial and Continuing Suitability Reports and Recommendations to the CIRC for review in accord with paragraph (II)(A)(3)(a).

---

[4] This provision did not apply until one year after these Guidelines' original effective date of January 8, 2001, when the first set of Continuing Suitability Reports and Recommendations was completed. Further, during the first three years that this provision is in effect, each CIRC may stagger the review of some long-term CIs in order to even out the number of files that must initially be reviewed. However, no later than four years after the original effective date of these Guidelines, all of the CIs who were registered for more than six consecutive years as of the original effective date of these Guidelines must be reviewed pursuant to this provision.

## B. REGISTRATION

After a Field Manager has approved an individual as suitable to be a CI, the individual shall be registered with that JLEA as a CI. In registering a CI, the JLEA shall, at a minimum, document or include the following in the CI's files:

1. a photograph of the CI;

2. the JLEA's efforts to establish the CI's true identity;

3. the results of a criminal history check for the CI;

4. the Initial Suitability Report and Recommendation;

5. any promises or benefits, and the terms of such promises or benefits, that are given a CI by a JLEA or any other law enforcement agency (if available to the JLEA);

6. any promises or benefits, and the terms of such promises or benefits, that are given a CI by any FPO or any state or local prosecuting office (if available to the JLEA); and

7. all information that is required to be documented in the CI's files pursuant to these Guidelines (e.g., the provision of the instructions set forth in the next paragraph).

## C. INSTRUCTIONS

1. In registering a CI, at least one agent of the JLEA, along with one additional agent or other law enforcement official present as a witness, shall review with the CI written instructions that state that:

   a. information provided by the CI to the JLEA must be truthful;

   b. the CI's assistance and the information provided are entirely voluntary;

   c. the United States Government will strive to protect the CI's identity but cannot guarantee that it will not be divulged;

   d. [if applicable:] the JLEA on its own cannot promise or agree to any immunity from prosecution or other consideration by a Federal Prosecutor's Office or a Court in exchange for the CI's cooperation, since the decision to confer any such benefit lies within the exclusive discretion

of the Federal Prosecutor's Office and the Court. However, the JLEA will consider (but not necessarily act upon) a request by the CI to advise the appropriate Federal Prosecutor's Office or Court of the nature and extent of his or her assistance to the JLEA;[5]

e. [if applicable:] the CI has not been authorized to engage in any criminal activity and has no immunity from prosecution for any unauthorized criminal activity;[6]

f. the CI must abide by the instructions of the JLEA and must not take or seek to take any independent action on behalf of the United States Government;

g. the CI is not an employee of the United States Government and may not represent himself or herself as such;

h. the CI may not enter into any contract or incur any obligation on behalf of the United States Government, except as specifically instructed and approved by the JLEA;

i. the JLEA cannot guarantee any rewards, payments, or other compensation to the CI;

j. in the event that the CI receives any rewards, payments, or other compensation from the JLEA, the CI is liable for any taxes that may be owed; and

---

[5] This instruction should be provided if there is any apparent issue of criminal liability or penalties that relates to the CI. Whether or not this instruction is given to a CI, the JLEA does not have any authority to make any promise or commitment that would prevent the government from prosecuting an individual, except as provided in paragraphs (I)(C) above and (III)(C) below, and a JLEA agent must avoid giving any person the erroneous impression that he or she has any such authority.

[6] This instruction should be provided to any CI who is not authorized to engage in otherwise illegal activity. See paragraph (III)(C)(4) for instructions that must be provided to a CI who is, in fact, authorized to engage in otherwise illegal conduct.

k. [if applicable:] no promises or commitments can be made, except by the Immigration and Naturalization Service, regarding the alien status of any person or the right of any person to enter or remain in the United States.[7]

2. The content and meaning of each of the foregoing instructional points must be clearly conveyed to the CI. Immediately after these instructions have been given, the agent shall require the CI to acknowledge his or her receipt and understanding of the instructions. The agent and the other law enforcement official shall document that the instructions were reviewed with the CI and that the CI acknowledged the instructions and his or her understanding of them. As soon as practicable thereafter, a Field Manager shall review and, if warranted, approve the documentation.

3. The instruction and documentation procedures shall be repeated whenever it appears necessary or prudent to do so, and in any event at least every twelve months.

## D. SPECIAL APPROVAL REQUIREMENTS

### 1. High Level Confidential Informants

a. Prior to utilizing an individual as a High Level Confidential Informant, a case agent of a JLEA shall first obtain the written approval of the CIRC. A Criminal Division representative on the CIRC who disagrees with a decision to approve the use of an individual as a High Level Confidential Informant may seek review of that decision pursuant to paragraph (I)(G).

b. In deciding whether to approve the use of a High Level Confidential Informant, the CIRC shall have access to any Initial or Completed Suitability Reports and Recommendations for the individual in question.

c. After a final decision has been made to approve the use of a High Level Confidential Informant, the CIRC shall consider whether to notify the Chief Federal Prosecutor of any FPO that is participating in the conduct of an investigation that is, or would be, utilizing the High Level Confidential Informant, or any FPO that has been, or would be, working with that individual in connection with a prosecution, of the decision to approve that individual as a High Level Confidential Informant. If the CIRC determines that no such notification shall be made, the reason or reasons for the determination shall be provided to the Criminal Division

---

[7] This instruction should be provided if there is any apparent issue of immigration status that relates to the CI and the JLEA is not the Immigration and Naturalization Service.

representatives on the CIRC. A Criminal Division representative on the CIRC who disagrees with a decision not to provide such notification may seek review of that decision pursuant to paragraph (I)(G).

2. **Individuals Under the Obligation of a Legal Privilege of Confidentiality or Affiliated with the Media**

   a. Prior to utilizing as a Confidential Informant an individual who is under the obligation of a legal privilege of confidentiality or affiliated with the media, a case agent of a JLEA shall first obtain the written approval of the CIRC. A Criminal Division representative on the CIRC who disagrees with a decision to approve the use of such an individual as a Confidential Informant may seek review of that decision pursuant to paragraph (I)(G).

   b. In deciding whether to approve the use as a Confidential Informant of an individual who is under the obligation of a legal privilege of confidentiality or affiliated with the media, the CIRC shall have access to any Initial or Completed Suitability Reports and Recommendations for the individual in question.

   c. After a final decision has been made to approve the use of an individual who is under the obligation of a legal privilege of confidentiality or affiliated with the media as a Confidential Informant, the CIRC shall consider whether to notify the Chief Federal Prosecutor of any FPO that is participating in the conduct of an investigation that is, or would be, utilizing the individual, or any FPO that has been, or would be, working with that individual in connection with a prosecution, of the decision to approve that individual as a Confidential Informant. If the CIRC determines that no such notification shall be made, the reason or reasons for the determination shall be provided to the Criminal Division representatives on the CIRC. A Criminal Division representative on the CIRC who disagrees with a decision not to provide such notification may seek review of that decision pursuant to paragraph (I)(G).

3. **Federal Prisoners, Probationers, Parolees, Detainees, and Supervised Releasees**

   a. Consistent with extant Department of Justice requirements, a JLEA must receive the approval of the Criminal Division's Office of Enforcement Operations ("OEO") prior to utilizing as a CI an individual who is in the custody of the United States Marshals Service or the Bureau of Prisons, or who is under Bureau of Prisons supervision. See U.S.A.M. § 9-21.050.

b. Prior to utilizing a federal probationer, parolee, or supervised releasee as a CI, a Field Manager of a JLEA shall determine if the use of that person in such a capacity would violate the terms and conditions of the person's probation, parole, or supervised release. If the Field Manger has reason to believe that it would violate such terms and conditions, prior to using the person as a CI, the Field Manager or his or her designee must obtain the permission of a federal probation, parole, or supervised release official with authority to grant such permission, which permission shall be documented in the CI's files. If such permission is denied or it is inappropriate for operational reasons to contact the appropriate federal official, the JLEA may seek to obtain authorization for the use of such individual as a CI from the Court then responsible for the individual's probation, parole, or supervised release, provided that the JLEA first consults with the FPO for that District.

c. In situations where a FPO is either participating in the conduct of an investigation by a JLEA in which a federal probationer, parolee, or supervised releasee would be utilized as a CI, or where a FPO would be working with a federal probationer, parolee, or supervised releasee in connection with a prosecution, the JLEA shall notify the attorney assigned to the matter prior to using the person as a CI.

**4. Current or Former Participants in the Witness Security Program**

a. Consistent with extant Department of Justice requirements, a JLEA must receive the approval of OEO and the sponsoring prosecutor (or his or her successor) prior to utilizing as a CI a current or former participant in the Federal Witness Security Program, provided further that the OEO will coordinate such matters with the United States Marshals Service. See U.S.A.M. § 9-21.800.

b. In situations where a FPO is either participating in the conduct of an investigation by a JLEA in which a current or former participant in the Witness Security Program would be utilized as a CI, or where a FPO would be working with a current or former participant in the Witness Security Program in connection with a prosecution, the JLEA shall notify the attorney assigned to the matter prior to using the person as a CI.

**5. State or Local Prisoners, Probationers, Parolees, or Supervised Releasees**

a. Prior to utilizing a state or local prisoner, probationer, parolee, or supervised releasee as a CI, a Field Manager of a JLEA shall determine if the use of that person in such a capacity would violate the terms and

conditions of the person's incarceration, probation, parole, or supervised release. If the Field Manger has reason to believe that it would violate such terms and conditions, prior to using the person as a CI, the Field Manager or his or her designee must obtain the permission of a state or local prison, probation, parole, or supervised release official with authority to grant such permission, which permission shall be documented in the CI's files. If such permission is denied or it is inappropriate for operational reasons to contact the appropriate state or local official, the JLEA may seek to obtain authorization for the use of such individual as a CI from the state or local Court then responsible for the individual's incarceration, probation, parole, or supervised release.

b. In situations where a FPO is either participating in the conduct of an investigation by a JLEA in which a state or local prisoner, probationer, parolee, or supervised releasee would be utilized as a CI, or where a FPO would be working with a state or local prisoner, probationer, parolee, or supervised releasee in connection with a prosecution, the JLEA shall notify the attorney assigned to the matter prior to using the person as a CI.

**6. Fugitives**

a. Except as provided below, a JLEA shall have no communication with a current or former CI who is a fugitive.

b. A JLEA is permitted to have communication with a current or former CI who is a fugitive:

(i) if the communication is part of a legitimate effort by that JLEA to arrest the fugitive; or

(ii) if approved, in advance whenever possible, by a Senior Field Manager of any federal, state, or local law enforcement agency that has a wanted record for the individual in the NCIC and, in the case of a federal warrant, by the FPO for the issuing District.

c. A JLEA that has communication with a fugitive must promptly report such communication to all federal, state, and local law enforcement agencies and other law enforcement agencies having a wanted record for the individual in the NCIC, and document those communications in the CI's files.

## III. RESPONSIBILITIES REGARDING REGISTERED CONFIDENTIAL INFORMANTS

### A. GENERAL PROVISIONS

#### 1. No Interference With an Investigation of a Confidential Informant

A JLEA agent must take the utmost care to avoid interfering with or impeding any criminal investigation or arrest of a CI. No agent shall reveal to a CI any information relating to an investigation of the CI. An agent shall not confirm or deny the existence of any investigation of the CI, unless authorized to do so by the Chief Federal Prosecutor; nor shall an agent agree to a request from a CI to determine whether the CI is the subject of any investigation.

#### 2. Prohibited Transactions and Relationships

a. A JLEA agent shall not: (i) exchange gifts with a CI; (ii) provide the CI with any thing of more than nominal value; (iii) receive any thing of more than nominal value from a CI; or (iv) engage in any business or financial transactions with a CI. Except as authorized pursuant to paragraph (III)(B) below, any exception to this provision requires the written approval of a Field Manager, in advance whenever possible, based on a written finding by the Field Manager that the event or transaction in question is necessary and appropriate for operational reasons. This written finding shall be maintained in the CI's files.

b. A Federal Law Enforcement agent shall not socialize with a CI except to the extent necessary and appropriate for operational reasons.

c. In situations where a FPO is either participating in the conduct of an investigation by a JLEA that is utilizing a CI, or working with a CI in connection with a prosecution, the JLEA shall notify the attorney assigned to the matter, in advance whenever possible, if the JLEA approves an exception under paragraph (III)(A)(2)(a) or if a Federal Law Enforcement agent socializes with a CI in a manner not permitted under paragraph (III)(A)(2)(b).

### B. MONETARY PAYMENTS

#### 1. General

Monies that a JLEA pays to a CI in the form of fees and rewards shall be commensurate with the value, as determined by the JLEA, of the information he or she provided or the

assistance he or she rendered to that JLEA. A JLEA's reimbursement of expenses incurred by a CI shall be based upon actual expenses incurred.

**2. Prohibition Against Contingent Payments**

Under no circumstances shall any payments to a CI be contingent upon the conviction or punishment of any individual.

**3. Approval for a Single Payment**

A single payment of between $2,500 and $25,000 per case to a CI must be authorized, at a minimum, by a JLEA's Senior Field Manager. A single payment in excess of $25,000 per case shall be made only with the authorization of the Senior Field Manager and the express approval of a designated senior headquarters official.

**4. Approval for Annual Payments**

Consistent with paragraph (III)(B)(3) above, payments by a JLEA to a CI that exceed an aggregate of $100,000 within a one-year period, as that period is defined by the JLEA, shall be made only with the authorization of the Senior Field Manager and the express approval of a designated senior headquarters official. The headquarters official may authorize additional aggregate annual payments in increments of $50,000 or less.

**5. Approval for Aggregate Payments**

Consistent with paragraphs (III)(B)(3)-(4), and regardless of the time frame, any payments by a JLEA to a CI that exceed an aggregate of $200,000 shall be made only with the authorization of the Senior Field Manager and the express approval of a designated senior headquarters official. After the headquarters official has approved payments to a CI that exceed an aggregate of $200,000, the headquarters official may authorize, subject to paragraph (III)(B)(4) above, additional aggregate payments in increments of $100,000 or less.

**6. Documentation of Payment**

The payment of any monies to a CI shall be witnessed by at least two law enforcement representatives. Immediately afer receiving a payment, the CI shall be required to sign or initial, and date, a written receipt.[8] At the time of the payment, the representatives shall advise the CI that the monies may be taxable income that must be reported to appropriate tax authorities. Thereafter, those representatives shall document the payment and the advice of taxability in the

[8] The CI may sign or initial the written receipt by using a pseudonym which has been previously approved and documented in the CI's files and designated for use by only one CI.

JLEA's files. The documentation of payment shall specify whether the payment is for information, services, or expenses.

### 7. Accounting and Reconciliation Procedures

Each JLEA shall establish accounting and reconciliation procedures to comply with these Guidelines. Among other things, these procedures shall reflect all monies paid to a CI subsequent to the issuance of these Guidelines.

### 8. Coordination with Prosecution

In situations where a FPO is either participating in the conduct of an investigation by a JLEA that is utilizing a CI, or working with a CI in connection with a prosecution, the JLEA shall coordinate with the attorney assigned to the matter, in advance whenever possible, the payment of monies to the CI pursuant to paragraphs (III)(B)(3)-(5) above.

## C. AUTHORIZATION OF OTHERWISE ILLEGAL ACTIVITY

### 1. General Provisions

a. A JLEA shall not authorize a CI to engage in any activity that otherwise would constitute a misdemeanor or felony under federal, state, or local law if engaged in by a person acting without authorization, except as provided in the authorization provisions in paragraph (III)(C)(2) below.

b. A JLEA is never permitted to authorize a CI to:

(i) participate in an act of violence;

(ii) participate in an act that constitutes obstruction of justice (e.g., perjury, witness tampering, witness intimidation, entrapment, or the fabrication, alteration, or destruction of evidence);

(iii) participate in an act designed to obtain information for the JLEA that would be unlawful if conducted by a law enforcement agent (e.g., breaking and entering, illegal wiretapping, illegal opening or tampering with the mail, or trespass amounting to an illegal search); or

(iv) initiate or instigate a plan or strategy to commit a federal, state, or local offense.

**2. Authorization**

a. Tier 1 Otherwise Illegal Activity must be authorized in advance and in writing for a specified period, not to exceed 90 days, by:

(i) a JLEA's Special Agent in Charge (or the equivalent); and

(ii) the appropriate Chief Federal Prosecutor.[9]

b. Tier 2 Otherwise Illegal Activity must be authorized in advance and in writing for a specified period, not to exceed 90 days, by a JLEA's Senior Field Manager.

c. For purposes of this paragraph, the "appropriate Chief Federal Prosecutor" is the Chief Federal Prosecutor that: (i) is participating in the conduct of an investigation by a JLEA that is utilizing that active CI, or is working with that active CI in connection with a prosecution; (ii) with respect to Otherwise Illegal Activity that would constitute a violation of federal law, would have primary jurisdiction to prosecute the Otherwise Illegal Activity; or (iii) with respect to Otherwise Illegal Activity that would constitute a violation only of state or local law, is located where the otherwise criminal activity is to occur.

**3. Findings**

a. The JLEA official who authorizes Tier 1 or 2 Otherwise Illegal Activity must make a finding, which shall be documented in the CI's files, that authorization for the CI to engage in the Tier 1 or 2 Otherwise Illegal Activity is –

(i) necessary either to -

(A) obtain information or evidence essential for the success of an investigation that is not reasonably available without such authorization, or

---

[9] Even without an express act of Congress authorizing the conduct at issue, it is within the power and the duty of federal prosecutors, as executive branch officers, to take reasonable measures to discharge the duties imposed on them as executive branch officers, and they will be immune from state action if they take such measures under color of federal law and in good faith.

(B) prevent death, serious bodily injury, or significant damage to property; and

(ii) that in either case the benefits to be obtained from the CI's participation in the Tier 1 or 2 Otherwise Illegal Activity outweigh the risks.

b. In making these findings, the JLEA shall consider, among other things:

(i) the importance of the investigation;

(ii) the likelihood that the information or evidence sought will be obtained;

(iii) the risk that the CI might misunderstand or exceed the scope of his authorization;

(iv) the extent of the CI's participation in the Otherwise Illegal Activity;

(v) the risk that the JLEA will not be able to supervise closely the CI's participation in the Otherwise Illegal Activity;

(vi) the risk of violence, physical injury, property damage, and financial loss to the CI or others; and

(vii) the risk that the JLEA will not be able to ensure that the CI does not profit from his or her participation in the authorized Otherwise Illegal Activity.

**4. Instructions**

a. After a CI is authorized to engage in Tier 1 or 2 Otherwise Illegal Activity, at least one agent of the JLEA, along with one additional agent or other law enforcement official present as a witness, shall review with the CI written instructions that state, at a minimum, that:

(i) the CI is authorized only to engage in the specific conduct set forth in the written authorization described above and not in any other illegal activity;

(ii) the CI's authorization is limited to the time period specified in the written authorization;

(iii) under no circumstance may the CI:

(A) participate in an act of violence;

(B) participate in an act that constitutes obstruction of justice (e.g., perjury, witness tampering, witness intimidation, entrapment, or the fabrication, alteration, or destruction of evidence);

(C) participate in an act designed to obtain information for the JLEA that would be unlawful if conducted by a law enforcement agent (e.g., breaking and entering, illegal wiretapping, illegal opening or tampering with the mail, or trespass amounting to an illegal search); or

(D) initiate or instigate a plan or strategy to commit a federal, state, or local offense;

(iv) if the CI is asked by any person to participate in any such prohibited conduct, or if he or she learns of plans to engage in such conduct, he or she must immediately report the matter to his or her contact agent; and

(v) participation in any prohibited conduct could subject the CI to full criminal prosecution.

b. Immediately after these instructions have been given, the CI shall be required to sign or initial, and date, a written acknowledgment of the instructions.[10] As soon as practicable thereafter, a Field Manager shall review and, if warranted, approve the written acknowledgment.

**5. Precautionary Measures**

Whenever a JLEA has authorized a CI to engage in Tier 1 or 2 Otherwise Illegal Activity, it must take all reasonable steps to: (a) supervise closely the illegal activities of the CI; (b) minimize the adverse effect of the authorized Otherwise Illegal Activity on innocent individuals; and (c) ensure that the CI does not profit from his or her participation in the authorized Otherwise Illegal Activity.

---

[10] The CI may sign or initial the written acknowledgment by using a pseudonym which has been previously approved and documented in the CI's files and designated for use by only one CI.

**6. Suspension of Authorization**

Whenever a JLEA cannot, for legitimate reasons unrelated to the CI's conduct (e.g., unavailability of the case agent), comply with the precautionary measures described above, it shall immediately: (a) suspend the CI's authorization to engage in Otherwise Illegal Activity until such time as the precautionary measures can be complied with; (b) inform the CI that his or her authorization to engage in any Otherwise Illegal Activity has been suspended until that time; and (c) document these actions in the CI's files.

**7. Revocation of Authorization**

a. If a JLEA has reason to believe that a CI has failed to comply with the specific terms of the authorization of Tier 1 or 2 Otherwise Illegal Activity, it shall immediately: (i) revoke the CI's authorization to engage in Otherwise Illegal Activity; (ii) inform the CI that he or she is no longer authorized to engage in any Otherwise Illegal Activity; (iii) comply with the notification requirement of paragraph (IV)(B) below; (iv) make a determination whether the CI should be deactivated pursuant to paragraph (V); and (v) document these actions in the CI's files.

b. Immediately afer the CI has been informed that he or she is no longer authorized to engage in any Otherwise Illegal Activity, the CI shall be required to sign or initial, and date, a written acknowledgment that he or she has been informed of this fact.[11] As soon as practicable thereafter, a Field Manager shall review and, if warranted, approve the written acknowledgment.

**8. Renewal and Expansion of Authorization**

a. A JLEA that seeks to re-authorize any CI to engage in Tier 1 or 2 Otherwise Illegal Activity after the expiration of the authorized time period, or after revocation of authorization, must first comply with the procedures set forth above in paragraphs (III)(C)(2)-(5).

---

[11] The CI may sign or initial the written acknowledgment by using a pseudonym which has been previously approved and documented in the CI's files and designated for use by only one CI. If the CI refuses to sign or initial the written acknowledgment, the JLEA agent who informed the CI of the revocation of authorization shall document that the CI has orally acknowledged being so informed and the Field Manager shall, as soon as practicable thereafter, review and, if warranted, approve the written documentation.

b. A JLEA that seeks to expand in any material way a CI's authorization to engage in Tier 1 or 2 Otherwise Illegal Activity by the JLEA must first comply with the procedures set forth above in paragraphs (III)(C)(2)-(5).

**9. Emergency Authorization**

a. In exceptional circumstances, a JLEA's Special Agent in Charge (or the equivalent) and the appropriate Chief Federal Prosecutor may orally authorize a CI to engage in Tier 1 Otherwise Illegal Activity without complying with the documentation requirements of paragraphs (III)(C)(2)-(4) above when they each determine that a highly significant and unanticipated investigative opportunity would be lost were the time taken to comply with these requirements. In such an event, the documentation requirements, as well as a written justification for the oral authorization, shall be completed within 48 hours of the oral approval and maintained in the CI's files.

b. In exceptional circumstances, a JLEA's Senior Field Manager may orally authorize a CI to engage in Tier 2 Otherwise Illegal Activity without complying with the documentation requirements of paragraphs (III)(C)(2)-(4) above when he or she determines that a highly significant and unanticipated investigative opportunity would be lost were the time taken to comply with these requirements. In such an event, the documentation requirements, as well as a written justification for the oral authorization, shall be completed within 48 hours of the oral approval and maintained in the CI's files.

**10. Designees**

A JLEA's Special Agent in Charge (or the equivalent) and the appropriate Chief Federal Prosecutor may, with the concurrence of each other, agree to designate particular individuals in their respective offices to carry out the approval functions assigned to them above in paragraphs (III)(C)(2)-(9).

## D. LISTING A CONFIDENTIAL INFORMANT IN AN ELECTRONIC SURVEILLANCE APPLICATION

1. A JLEA shall not name a CI as a named interceptee or a violator in an affidavit in support of an application made pursuant to 18 U.S.C. § 2516 for an electronic surveillance order unless the JLEA believes that: (a) omitting the name of the CI from the affidavit would endanger that person's life or otherwise jeopardize an ongoing investigation; or (b) the CI is a bona fide subject of the investigation based on his or her suspected involvement in unauthorized criminal activity.

2. In the event that a CI is named in an electronic surveillance affidavit under paragraph (III)(D)(1) above, the JLEA must inform the Federal prosecutor making the application and the Court to which the application is made of the actual status of the CI.

## IV. SPECIAL NOTIFICATION REQUIREMENTS

### A. NOTIFICATION OF INVESTIGATION OR PROSECUTION

1. When a JLEA has reasonable grounds to believe that a current or former CI is being prosecuted by, is the target of an investigation by, or is expected to become a target of an investigation by a FPO for engaging in alleged felonious criminal activity, a Special Agent in Charge (or the equivalent) of the JLEA must immediately notify the Chief Federal Prosecutor of that individual's status as a current or former CI.[12]

2. Whenever such a notification is provided, the Chief Federal Prosecutor and Special Agent in Charge (or the equivalent), with the concurrence of each other, shall notify any other federal, state or local prosecutor's offices or law enforcement agencies that are participating in the investigation or prosecution of the CI.

### B. NOTIFICATION OF UNAUTHORIZED ILLEGAL ACTIVITY

1. Whenever a JLEA has reasonable grounds to believe that a CI who is currently authorized to engage in specific Tier 1 or 2 Otherwise Illegal Activity has engaged in unauthorized criminal activity, or whenever a JLEA knows that a CI who has no current authorization to engage in any Tier 1 or 2 Otherwise Illegal Activity has engaged in any criminal activity, a Special Agent in Charge of the JLEA (or the equivalent) shall immediately notify the following Chief Federal Prosecutors of the CI's criminal activity and his or her status as a CI:

   a. the Chief Federal Prosecutor whose District is located where the criminal activity primarily occurred, unless a state or local prosecuting office in that District has filed charges against the CI for the criminal activity and there clearly is no basis for federal prosecution in that District by the Chief Federal Prosecutor;

---

[12] A target is "a person as to whom the prosecutor or the grand jury has substantial evidence linking him or her to the commission of a crime and who, in the judgment of the prosecutor, is a putative defendant." U.S.A.M. § 9-11.151.

b. the Chief Federal Prosecutor, if any, whose District is participating in the conduct of an investigation that is utilizing that active CI, or is working with that active CI in connection with a prosecution; and

c. the Chief Federal Prosecutor, if any, who authorized the CI to engage in Tier 1 Otherwise Illegal Activity pursuant to paragraph (III)(C)(2)(a) above.[13]

2. Whenever such notifications are provided, the Chief Federal Prosecutor(s) of the FPOs and the Special Agent in Charge (or the equivalent), with the concurrence of each other, shall notify any state or local prosecutor's office that has jurisdiction over the CI's criminal activity, and that has not already filed charges against the CI for the criminal activity, of the fact that the CI has engaged in such criminal activity. The Chief Federal Prosecutor(s) and the Special Agent in Charge (or the equivalent) are not required, but may with the concurrence of each other, also notify the state and local prosecutor's office of the person's status as a CI.

## C. NOTIFICATION REGARDING CERTAIN FEDERAL JUDICIAL PROCEEDINGS

Whenever a JLEA has reasonable grounds to believe that: (1) a current or former CI has been called to testify by the prosecution in any federal grand jury or judicial proceeding; (2) the statements of a current or former CI have been, or will be, utilized by the prosecution in any federal judicial proceeding; or (3) a federal prosecutor intends to represent to a Court or jury that a current or former CI is or was a co-conspirator or other criminally culpable participant in any criminal activity, a Special Agent in Charge (or the equivalent) of the JLEA shall immediately notify the Chief Federal Prosecutor for that proceeding of the individual's status as a current or former CI.

## D. PRIVILEGED OR EXCULPATORY INFORMATION

1. In situations where a FPO is either participating in the conduct of an investigation by a JLEA that is utilizing a CI, or working with a CI in connection with a prosecution, the JLEA shall notify the attorney assigned to the matter, in advance whenever possible, if the JLEA has reasonable grounds to believe that a CI will obtain or provide information that is subject to, or arguably subject to, a legal privilege of confidentiality belonging to someone other than the CI.

---

[13] Whenever such notifications to FPOs are provided, the JLEA must also comply with the Continuing Suitability requirements described above in paragraph (II)(A)(2).

2. If the JLEA has reasonable grounds to believe that a current or former CI has information that is exculpatory as to a person who is expected to become a target of an investigation, or as to a target of an investigation, or as to a defendant (including a convicted defendant), the JLEA shall notify the Chief Federal Prosecutor responsible for the investigation or prosecution of such exculpatory information.

### E. RESPONDING TO REQUESTS FROM CHIEF FEDERAL PROSECUTORS REGARDING A CONFIDENTIAL INFORMANT

If a Chief Federal Prosecutor seeks information from a Special Agent in Charge (or the equivalent) as to whether a particular individual is a current or former CI, and states the specific basis for his or her request, the Special Agent in Charge (or the equivalent) shall provide such information promptly. If the Special Agent in Charge (or the equivalent) has an objection to providing such information based on specific circumstances of the case, he or she shall explain the objection to the Chief Federal Prosecutor making the request and any remaining disagreement as to whether the information should be provided shall be resolved pursuant to paragraph (I)(G).

### F. FILE REVIEWS

Whenever a JLEA discloses any information about a CI to a FPO pursuant to paragraphs (IV)(A)-(E), the Special Agent in Charge (or the equivalent) and the Chief Federal Prosecutor shall consult to facilitate any review and copying of the CI's files by the Chief Federal Prosecutor that might be necessary for the Chief Federal Prosecutor to fulfill his or her office's disclosure obligations.

### G. DESIGNEES

A Special Agent in Charge (or the equivalent) and a Chief Federal Prosecutor may, with the concurrence of each other, agree to designate particular individuals in their respective offices to carry out the functions assigned to them in paragraphs (IV)(A)-(F).

## V. DEACTIVATION OF CONFIDENTIAL INFORMANTS

### A. GENERAL PROVISIONS

A JLEA that determines that a CI should be deactivated for cause or for any other reason shall immediately:

1. deactivate the individual;

2. document the reasons for the decision to deactivate the individual as a CI in the CI's files;

3. if the CI can be located, notify the CI that he or she has been deactivated as a CI and obtain documentation that such notification was provided in the same manner as set forth in paragraph (II)(C)(2); and

4. if the CI was authorized to engage in Tier 1 or Tier 2 Otherwise Illegal Activity pursuant to paragraph (III)(C)(2)(a)-(b), revoke that authorization under the provisions of paragraph (III)(C)(7).

## B. DELAYED NOTIFICATION TO A CONFIDENTIAL INFORMANT

A JLEA may delay providing the notification to the CI described above in Paragraph (V)(A)(3) during the time such notification might jeopardize an ongoing investigation or prosecution or might cause the flight from prosecution of any person. Whenever a decision is made to delay providing a notification, that decision, and the reasons supporting it, must be documented in the CI's files.

## C. CONTACTS WITH FORMER CONFIDENTIAL INFORMANTS DEACTIVATED FOR CAUSE

Absent exceptional circumstances that are approved by a Senior Field Manager, in advance whenever possible, an agent of a JLEA shall not initiate contacts with, or respond to contacts from, a former CI who has been deactivated for cause. When granted, such approval shall be documented in the CI's files.

## D. COORDINATION WITH PROSECUTORS

In situations where a FPO is either participating in the conduct of an investigation by a JLEA that is utilizing a CI, or working with a CI in connection with a prosecution, the JLEA shall coordinate with the attorney assigned to the matter, in advance whenever possible, regarding any of the decisions described in paragraphs (V)(A)-(C).

Date: May 30, 2002

John Ashcroft
Attorney General

# THE ATTORNEY GENERAL'S GUIDELINES ON FEDERAL BUREAU OF INVESTIGATION UNDERCOVER OPERATIONS

## PREAMBLE

The following Guidelines on the use of undercover activities and operations by the Federal Bureau of Investigation (FBI) are issued under the authority of the Attorney General as provided in sections 509, 510, and 533 of title 28, United States Code. They apply to investigations conducted by the FBI pursuant to the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations.

## TABLE OF CONTENTS

## I. INTRODUCTION

The use of undercover techniques, including proprietary business entities, is essential to the detection, prevention, and prosecution of white collar crimes, public corruption, terrorism, organized crime, offenses involving controlled substances, and other priority areas of investigation. However, these techniques inherently involve an element of deception and may require cooperation with persons whose motivation and conduct are open to question, and so should be carefully considered and monitored.

## II. DEFINITIONS

A. **"Undercover Activities"** means any investigative activity involving the use of an assumed name or cover identity by an employee of the FBI or another Federal, state, or local law enforcement organization working with the FBI.

B. **"Undercover Operation"** means an investigation involving a series of related undercover activities over a period of time by an undercover employee. For purposes of these Guidelines, a "series of related undercover activities" generally consists of more than three separate substantive contacts by an undercover employee with the individual(s) under investigation. However, undercover activity involving sensitive or fiscal circumstances constitutes an undercover operation regardless of the number of contacts involved. A contact is "substantive" if it is a communication with another person, whether by oral, written, wire, or electronic means, which includes information of investigative interest. Mere incidental contact, e.g., a conversation that establishes an agreed time and location for another meeting, is not a substantive contact within the meaning of these Guidelines.

NOTE: In the context of online communications, such as e-mail and Internet Relay Chat (IRC), multiple transmissions or e-mail messages can constitute one contact, much like a series of verbal exchanges can comprise a single conversation. Factors to be considered in determining whether multiple online transmissions constitute a single contact or multiple contacts include the time between transmissions, the number of transmissions, the number of interruptions, topical transitions, and the media by which the communications are exchanged (i.e., e-mail versus IRC). For more detailed discussion, see the Online Investigative Principles for Federal Law Enforcement Agents, Principle 6, Section C.

C. **"Undercover Employee"** means any employee of the FBI, or employee of a Federal, state, or local law enforcement agency working under the direction and control of the FBI in a particular investigation, whose relationship with the FBI is concealed from third parties in the course of an investigative operation by the maintenance of a cover or alias identity.

D. **"Proprietary"** means a sole proprietorship, partnership, corporation, or other business entity operated on a commercial basis, which is owned, controlled, or operated wholly or in part on behalf of the FBI, and whose relationship with the FBI is concealed from third parties.

E. **"Appropriate Federal Prosecutor"** means a United States Attorney or Section Chief in the Criminal Division of the Department of Justice (DOJ).

F. **"Joint Undercover Operation"** means an undercover operation conducted jointly by the FBI and another law enforcement agency, except that an operation in which FBI participation is confined to contribution of limited financial or equipment resources or technical advice does not constitute a joint undercover operation.

## III. GENERAL AUTHORITY AND PURPOSE

The FBI may engage in undercover activities and undercover operations pursuant to these Guidelines that are appropriate to carry out its law enforcement responsibilities, including the conduct of preliminary inquiries, general crimes investigations, and criminal intelligence investigations. In preliminary inquiries, these methods may be used to further the objective of inquiry into possible criminal activities by individuals or groups to determine whether a full investigation is warranted. In general crimes investigations, these methods may be used to further the investigative objectives of preventing, solving, and prosecuting crimes. In criminal intelligence investigations – i.e., racketeering enterprise investigations and terrorism enterprise investigations – these methods may be used to further the investigative objective of ascertaining such matters as the membership, finances, geographical dimensions, past and future activities, and goals of the enterprise under investigation, with a view to the longer range objectives of detection, prevention, and prosecution of the criminal activities of the enterprise.

These guidelines do not apply to investigations utilizing confidential informants, cooperating witnesses or cooperating subjects, unless the investigation also utilizes an undercover employee. However, the FBI, through the development of internal policy, may choose to apply these Guidelines to certain confidential informant, cooperating witness, and cooperating subject operations by referring such matters to the Undercover Review Committee pursuant to Section IV.D(6).

The FBI may participate in joint undercover activities with other law enforcement agencies and may operate a proprietary to the extent necessary to maintain an operation's cover or effectiveness. Joint undercover operations are to be conducted pursuant to these Guidelines. However, if a joint undercover operation is under the direction and control of another federal law enforcement agency and is approved through a sensitive operations review process substantially comparable to the process under these Guidelines, the other agency's process may be relied on in lieu of the process under these Guidelines. In any undercover activity or operation in which an FBI undercover employee participates, Sections IV.H and VI.A-B of these Guidelines shall apply, regardless of which agency directs and controls the operation.

## IV. AUTHORIZATION OF UNDERCOVER OPERATIONS

### A. GENERAL APPROVAL STANDARDS

Any official considering approval or authorization of a proposed undercover application shall weigh the risks and benefits of the operation, giving careful consideration to the following factors:

(1) The risk of personal injury to individuals, property damage, financial loss to persons or businesses, damage to reputation, or other harm to persons;

(2) The risk of civil liability or other loss to the Government;

(3) The risk of invasion of privacy or interference with privileged or confidential relationships and any potential constitutional concerns or other legal concerns;

(4) The risk that individuals engaged in undercover operations may become involved in illegal conduct restricted in Section IV.H below; and

(5) The suitability of Government participation in the type of activity that is expected to occur during the operation.

### B. UNDERCOVER OPERATIONS WHICH MAY BE AUTHORIZED BY THE SPECIAL AGENT IN CHARGE (SAC)

(1) The establishment, extension, or renewal of all undercover operations to be supervised by a given field office must be approved by the SAC. If the undercover operation does not involve any of the factors listed in Section IV.C below, this approval shall constitute authorization for the operation. Approval requires a written determination, stating supporting facts and circumstances, that:

(a) Initiation of investigative activity regarding the alleged criminal conduct or criminal enterprise is warranted under any applicable departmental guidelines;

(b) The proposed undercover operation appears to be an effective means of obtaining evidence or necessary information. This finding should include a statement of what prior investigation has been conducted and what chance the operation has of obtaining evidence or necessary information concerning the alleged criminal conduct or criminal enterprise;

NOTE: The gathering of evidence and information through undercover operations furthers the investigative objectives of detecting, preventing, and prosecuting crimes. See Sections I and III above. In furthering these objectives, the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism

Enterprise Investigations (Part I) state that "[t]he 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." As with other investigative techniques, Special Agents in Charge should be guided by this principle in considering and approving undercover operations. The principle, as noted, applies with particular force where the undercover operation is directed to gathering information that will help to solve and prosecute terrorist offenses or prevent the future commission of acts of terrorism.

(c) The undercover operation will be conducted with minimal intrusion consistent with the need to collect the evidence or information in a timely and effective manner;

(d) Approval for the use of any confidential informant has been obtained as required by the Attorney General's Guidelines Regarding the Use of Confidential Informants;

(e) Any foreseeable participation by an undercover employee in illegal activity that can be approved by the SAC on his or her own authority is justified by the factors noted in paragraph H; and

(f) If there is no present expectation of the occurrence of any of the sensitive or fiscal circumstances listed in paragraph C, a statement to that effect.

(2) Undercover operations may be authorized pursuant to this subsection for up to six months and continued upon renewal for an additional six-month period, for a total of no more than one year. Undercover operations initiated pursuant to this subsection may not involve the expenditure of more than $50,000 ($100,000 in drug cases of which a maximum of $50,000 is for operational expenses), or such other amount that is set from time to time by the Director, without approval from FBI Headquarters (FBIHQ).

(3) The SAC may delegate the responsibility to authorize the establishment, extension, or renewal of undercover operations to designated Assistant Special Agents in Charge. The delegation of this responsibility by the SAC should be in writing and maintained in the appropriate field office. However, all undercover operations which must be authorized at FBIHQ must be approved by the SAC.

(4) A copy of all written approvals described in (1) above shall be forwarded promptly to FBIHQ.

## C. OPERATIONS WHICH MUST BE APPROVED AT FBIHQ

(1) Fiscal Circumstances

In all undercover operations involving the fiscal circumstances set out below, the SAC shall submit an application to FBIHQ in accordance with Section IV.F below. A recommendation for authorization may be forwarded directly to the Director or designated Assistant Director or, in operations involving only fiscal circumstances (a)-(c), to the designated Deputy Assistant Director for final review and authorization, provided that the approval levels conform to all applicable laws.

Applications for approval of undercover operations referred to FBIHQ only because of fiscal circumstances need not be considered or approved by the Undercover Review Committee.

For purpose of these Guidelines, an undercover operation involves fiscal circumstances if there is a reasonable expectation that the undercover operation will –

(a) Require the purchase or lease of property, equipment, buildings, or facilities; the alteration of buildings or facilities; a contract for construction or alteration of buildings or facilities; or prepayment of more than one month's rent;

NOTE: The purchase, rental, or lease of property using an assumed name or cover identity to facilitate a physical or technical surveillance is not an undercover operation for purposes of these Guidelines. However, since the expenditure of appropriated funds is involved, approval must be obtained from FBIHQ in conformance with applicable laws.

(b) Require the deposit of appropriated funds or proceeds generated by the undercover operation into banks or other financial institutions;

(c) Use the proceeds generated by the undercover operation to offset necessary and reasonable expenses of the operation;

(d) Require a reimbursement, compensation, or indemnification agreement with cooperating individuals or entities for services or losses incurred by them in aid of the operation (any such agreement entered into with third parties must be reviewed by the FBI's Office of the General Counsel and Office of the Chief Contracting Officer); or

(e) Exceed the limitations on duration or commitment of resources established by the Director for operations initiated at the field office level.

(2) Sensitive Circumstances

In all undercover operations involving any sensitive circumstances listed below, the SAC shall submit an application to FBIHQ in accordance with paragraph F below. The application shall be reviewed by appropriate supervisory personnel at FBIHQ and, if favorably recommended, sent to the Undercover Review Committee for consideration. The application shall then be forwarded to the Director or a designated Assistant Director, who may approve or disapprove the application.

For purposes of these Guidelines, sensitive circumstances are involved if there is a reasonable expectation that the undercover operation will involve –

(a) an investigation of possible criminal conduct by any elected or appointed official, or political candidate, for a judicial, legislative, management, or executive-level position of trust in a Federal, state, or local governmental entity or political subdivision thereof;

(b) an investigation of any public official at the Federal, state, or local level in any matter involving systemic corruption of any governmental function;

(c) an investigation of possible criminal conduct by any foreign official or government, religious organization, political organization, or the news media;

NOTE: There are some circumstances involving officials in judicial, legislative, management, or executive-level positions which may logically be considered nonsensitive. In such instances, the Section Chief, Integrity in Government/Civil Rights Section, Criminal Investigative Division, FBIHQ, who is a member of the Criminal Undercover Operations Review Committee and has a national perspective on matters involving public officials, must be consulted for a determination as to whether the undercover operation should be presented to the Undercover Review Committee.

(d) Engaging in activity having a significant effect on or constituting a significant intrusion into the legitimate operation of a Federal, state, or local governmental entity;

(e) Establishing, acquiring, or operating a proprietary;

(f) Providing goods or services which are essential to the commission of a crime, which goods and services are reasonably unavailable to a subject of the investigation except from the Government;

(g) Activity by an undercover employee that is proscribed by Federal, state, or local law as a felony or that is otherwise a serious crime – but not including the purchase of stolen or contraband goods; the delivery or sale by the Government of

stolen property whose ownership cannot be determined; the controlled delivery of drugs which will not enter commerce; the conduct of no more than five money laundering transactions, not to exceed a maximum aggregate amount of $1 million; the payment of bribes which are not included in the other sensitive circumstances; or the making of false representations to third parties in concealment of personal identity or the true ownership of a proprietary (this exemption does not include any statement under oath or the penalties of perjury – see paragraph H below);

NOTE: Some of the above activities – for example, the controlled delivery of drugs, bribe payments, and certain transactions that involve depositing funds into banks or other financial institutions – are subject to specific review and approval procedures. These matters must be coordinated with FBIHQ.

(h) A significant risk that a person participating in an undercover operation will be arrested or will supply falsely sworn testimony or false documentation in any legal or administrative proceeding (see paragraph H below);

(i) Attendance at a meeting or participation in communications between any individual and his or her lawyer;

(j) A significant risk that a third party will enter into a professional or confidential relationship with a person participating in an undercover operation who is acting as an attorney, physician, clergyman, or member of the news media;

(k) A request to an attorney, physician, member of the clergy, or other person for information that would ordinarily be privileged or to a member of the news media concerning an individual with whom the news person is known to have a professional or confidential relationship;

(l) Participation in the activities of a group under investigation as part of a terrorism enterprise investigation or recruiting a person from within such a group as an informant;

(m) A significant risk of violence or physical injury to individuals or a significant risk of financial loss;

(n) Activities which create a realistic potential for significant claims against the United States arising in tort, contract, or for compensation for the "taking" of property, or a realistic potential for significant claims against individual government employees alleging constitutional torts; or

(o) Untrue representations by a person participating in the undercover operation concerning the activities or involvement of any third person without that individual's knowledge or consent.

## D. CRIMINAL UNDERCOVER OPERATIONS REVIEW COMMITTEE (UNDERCOVER REVIEW COMMITTEE)

(1) The Undercover Review Committee shall consist of appropriate employees of the FBI designated by the Director and Criminal Division attorneys designated by the Assistant Attorney General in charge of the Criminal Division, DOJ, to be chaired by a designee of the Director.

(2) When an application from a SAC for approval of an undercover operation involving sensitive circumstances specified in paragraph C(2) is received by FBIHQ, upon recommendation by the FBIHQ substantive section, the Committee members will meet to review the application. Criminal Division members of the Committee may consult with appropriate FBI personnel, senior DOJ officials, and the United States Attorney as deemed appropriate. The Committee shall submit the application to the Director or designated Assistant Director with a recommendation for approval or disapproval of the request and any recommended changes or amendments to the proposal.

(3) In addition to the considerations contained in Section IV.A above, the Committee shall also examine the application to determine whether adequate measures have been taken to minimize the incidence of sensitive circumstances and reduce the risks of harm and intrusion that are created by such circumstances. If the Committee recommends approval of an undercover operation, the recommendation shall include a brief written statement explaining why the operation merits approval in light of the anticipated occurrence of sensitive circumstances.

(4) The Committee shall recommend approval of an undercover operation only upon reaching a consensus, provided that:

(a) If one or more of the designees of the Assistant Attorney General in charge of the Criminal Division does not join in a recommendation for approval of a proposed operation because of legal, ethical, prosecutive, or departmental policy considerations, the designee shall promptly advise the Assistant Attorney General and no further action shall be taken on the proposal until the designated Assistant Director has had an opportunity to consult with the Assistant Attorney General; and

(b) If, upon consultation, the Assistant Attorney General disagrees with a decision by the designated Assistant Director to approve the proposed operation, no further action shall be taken on the proposal without the approval of the Deputy Attorney General or the Attorney General.

(5) The Committee should consult the Office of the General Counsel of the FBI and the Office of Legal Counsel or other appropriate division or office at DOJ about significant unsettled legal questions concerning authority for, or the conduct of, a proposed undercover operation.

(6) The Director, Assistant Attorney General, or other official designated by them may refer any sensitive investigative matter, including informant, cooperating witness, and cooperating subject operations, to the Undercover Review Committee for advice, recommendation or comment, regardless of whether an undercover operation is involved. A SAC may, consistent with FBI policy, submit an undercover operation for review by FBIHQ and the Undercover Review Committee, regardless of whether the sensitive circumstances listed in these Guidelines are present.

(7) The United States Attorney, SAC or any member of their staffs, may attend the Undercover Review Committee in order to advocate for the approval of an undercover operation.

(8) If the SAC and the United States Attorney jointly disagree with any stipulation set by the Undercover Review Committee regarding the approval of an undercover operation, they may consult with the chairman of the Committee who may schedule a meeting of the committee to reconsider the issue in question.

(9) At any time during the undercover operation the SAC can appeal any FBIHQ decision directly to the Assistant Director. Likewise, the United States Attorney can appeal directly to the Assistant Attorney General, Criminal Division, or the Deputy Attorney General as appropriate.

## E. APPROVAL BY THE DIRECTOR, DEPUTY DIRECTOR, DESIGNATED EXECUTIVE ASSISTANT DIRECTOR, OR DESIGNATED ASSISTANT DIRECTOR

A designated Assistant Director may approve an undercover operation considered by the Undercover Review Committee, unless the investigation involves sensitive circumstance (1) or (m). Except in the limited circumstances described in paragraph I below, only the Director, the Deputy Director, or a designated Executive Assistant Director may approve a proposed operation if a reasonable expectation exists that:

(1) The undercover operation will be used to participate in the activities of a group under investigation as part of a terrorism enterprise investigation or to recruit a person from within such a group as an informant (sensitive circumstance (l)); or

(2) There may be a significant risk of violence or personal injury to individuals or a significant risk of financial loss (sensitive circumstance (m)).

## F. APPLICATION/NOTIFICATION TO FBIHQ

(1) Application to FBIHQ must be made for any undercover operation requiring FBIHQ approval. Each application shall include:

(a) The written SAC approval described in paragraph B(1) above;

(b) A description of the proposed operation and the particular cover to be employed; any informants or other cooperating persons who will assist in the operation, including background information, arrest record, and plea agreements; the particular offense or criminal enterprise under investigation; and any individuals known to be involved;

(c) A statement of the period of time for which the operation would be maintained;

(d) A description of how the requirements concerning any inducements to be offered as discussed in Section V.B. below have been met; and

(e) A statement of proposed expenses.

(2) Applications for approval of undercover operations involving sensitive circumstances listed in paragraph C(2) shall also include the following information:

(a) A statement of which circumstances are reasonably expected to occur, what the facts are likely to be, and why the undercover operation merits approval in light of the circumstances, including:

(i) For undercover operations involving sensitive circumstance (g), a statement why the participation in otherwise illegal activity is justified under the requirements of paragraph H below; and

(ii) For undercover operations involving sensitive circumstance (l), a statement why the infiltration or recruitment is necessary, a description of procedures to minimize any acquisition, retention, and dissemination of information that does not relate to the matter under investigation or to other authorized investigative activity, and an explanation of how any potential constitutional concerns and any other legal concerns have been addressed.

(b) A letter from the appropriate Federal prosecutor indicating that he or she has reviewed the proposed operation, including the sensitive circumstances reasonably expected to occur, agrees with the proposal and its legality, and will prosecute any meritorious case that has developed. The letter should include a

finding that the proposed investigation would be an appropriate use of the undercover technique and that the potential benefits in detecting, preventing, or prosecuting criminal activity outweigh any direct costs or risks of other harm.

(3) An application for the extension or renewal of an undercover operation should describe the results obtained from the operation or explain any failure to obtain significant results and, where sensitive circumstances are involved, should include a letter from the appropriate Federal prosecutor favoring the extension or renewal of authority.

(4) The FBI shall immediately notify the Deputy Attorney General whenever FBIHQ disapproves an application for approval of an undercover operation and whenever the Undercover Review Committee is unable to reach consensus concerning an application.

## G. DURATION OF AUTHORIZATION

(1) An undercover operation approved by FBIHQ may not continue longer than is necessary to achieve the objectives specified in the authorization, nor in any event longer than six months, without new authorization to proceed, except pursuant to subparagraph (3) below.

(2) If there is significant change in either the direction or objectives of an undercover operation approved by FBIHQ, the operation must be reviewed by the Undercover Review Committee to determine whether a new authorization is necessary.

(3) An undercover operation which requires review by the Undercover Review Committee may be initiated or extended on an interim basis by the designated Assistant Director in the event of exigent circumstances, for a period not to exceed 30 days. In the case of an initial authorization, budget enhancement, or change in focus, the interim authority must be ratified by the Undercover Review Committee at its next scheduled meeting.

(4) An undercover operation initially authorized by the SAC must be reauthorized by a designated Assistant Director, pursuant to Section IV.C-F, if it lasts longer than 12 months or involves the expenditure of more than $50,000 ($100,000 in drug cases of which a maximum of $50,000 is for operational expenses), or such other amount that is set from time to time by the Director. No undercover operation approved at the field office level may continue for more than one year without obtaining approval at FBIHQ.

(5) An undercover operation approved by an SAC is deemed to commence on the date approved, not on the date covert activity is begun.

(6) Among the factors to be considered in a determination by any approving official of whether an undercover operation should be renewed or extended are:

(a) The extent to which the operation has produced the results anticipated when it was established;

(b) The potential for future success beyond that initially targeted;

(c) The extent to which the investigation can continue without exposing the undercover operation; and

(d) The extent to which continuation of the investigation may cause injury, financial or otherwise, to innocent parties.

## H. PARTICIPATION IN OTHERWISE ILLEGAL ACTIVITY BY UNDERCOVER EMPLOYEES

Except when authorized pursuant to these Guidelines, no undercover employee shall engage in any activity that would constitute a violation of Federal, state, or local law if engaged in by a private person acting without authorization. For purposes of these Guidelines, such activity is referred to as otherwise illegal activity.

(1) Justification: No official shall recommend or approve participation by an undercover employee in otherwise illegal activity unless the participation is justified:

(a) to obtain information or evidence necessary for the success of the investigation and not reasonably available without participation in the otherwise illegal activity;

(b) to establish or maintain credibility of a cover identity; or

(c) to prevent death or serious bodily injury.

(2) Minimization: The FBI shall take reasonable steps to minimize the participation of an undercover employee in any otherwise illegal activity.

(3) Prohibitions: An undercover employee shall not:

(a) participate in any act of violence except in self-defense;

(b) initiate or instigate any plan to commit criminal acts except in accordance with Section V (concerning avoidance of entrapment) below; or

(c) participate in conduct which would constitute unlawful investigative techniques (e.g., illegal wiretapping, illegal mail openings, breaking and entering, or trespass amounting to an illegal search).

(4) Self-Defense: Nothing in these Guidelines prohibits an undercover employee from taking reasonable measures of self-defense in an emergency to protect his or her own life or the lives of others against wrongful force. Such measures shall be reported to the appropriate Federal prosecutor and FBIHQ, who shall inform the Assistant Attorney General for the Criminal Division as soon as possible.

(5) Authorization:

(a) The SAC must approve all undercover operations and activities, including those which contemplate participation in otherwise illegal activity. This approval shall constitute authorization of:

(i) otherwise illegal activity which is a misdemeanor or similar minor crime under Federal, state, or local law;

(ii) consensual monitoring, even if a crime under local law;

(iii) the purchase of stolen or contraband goods;

(iv) the delivery or sale of stolen property which cannot be traced to the rightful owner;

(v) the controlled delivery of drugs which will not enter commerce;

(vi) the payment of bribes which is not included in the sensitive circumstances;

(vii) the making of false representations to third parties in concealment of personal identity or the true ownership of a proprietary (but not any statement under oath or the penalties of perjury, which must be authorized pursuant to subparagraph (b) below); and

(viii) conducting no more than five money laundering transactions, not to exceed a maximum aggregate amount of $1 million.

(b) Participation in otherwise illegal activity which is a felony or its equivalent under Federal, state, or local law and which is not otherwise excepted under Section IV.C(2)(g) above, requires additional authorization by the Assistant Director after review by the Undercover Review Committee. See Section IV.E.

(c) Participation in otherwise illegal activity which involves a significant risk of violence or physical injury requires authorization by the Director, Deputy Director, or designated Executive Assistant Director after review by the Undercover Review Committee. See Section IV.E.

(d) If an undercover employee believes it to be necessary and appropriate under the standards set out in paragraph H(1) above, to participate in otherwise illegal activity that was not foreseen or anticipated, every effort should be made to consult with the SAC, who shall seek emergency interim authority from the designated Assistant Director, and review by the Undercover Review Committee if possible, or, if necessary, may provide emergency authorization under paragraph I below. If consultation is impossible, and the undercover employee concludes that there is an immediate and grave threat to life, physical safety, or property, the undercover employee may participate in the otherwise illegal activity, so long as he does not take part in and makes every effort to prevent any act of violence. A report to the SAC shall be made as soon as possible, who shall submit a written report to FBIHQ, which shall promptly inform the Undercover Review Committee. A decision by an undercover employee to participate in otherwise illegal activity under this subsection may be retroactively authorized if appropriate.

(e) If an undercover operation results in violence in the course of criminal activity, and an undercover employee, informant, or cooperating witness has participated in any manner in the criminal activity, the SAC shall immediately inform the appropriate Federal prosecutor and FBIHQ, which shall inform the Assistant Attorney General in charge of the Criminal Division as soon as possible.

## I. INTERIM/EMERGENCY AUTHORIZATION

(1) In situations which require the prior written authorization of the SAC, the SAC may orally approve an undercover operation when he or she determines that a significant investigative opportunity would be lost were the time taken to prepare a written authorization. The required written authorization, with the justification for the oral approval included, shall be prepared promptly and forwarded to FBIHQ.

(2) Emergency interim authorization procedures are in place within FBIHQ that provide for expeditious review and authorization of a proposed undercover operation. See paragraph G(3). If the SAC concludes that a situation exists which makes even this expedited procedure too lengthy, in any of the following situations, the SAC may authorize the undercover operation:

(a) In situations which would otherwise require approval by the designated Assistant Director, the SAC may approve an undercover operation when he or she determines that without immediate initiation, extension, or renewal of an operation, life, property, or personal safety of individuals would be placed in serious danger.

(b) In situations which involve sensitive circumstance (l) or (m), the SAC may approve an undercover operation when he or she determines that the initiation, extension, or renewal of an operation is imperative to protect life or prevent serious injury.

(c) In situations which involve sensitive circumstance (l), or other investigative activity relating to terrorism, the SAC may approve an undercover operation when he or she determines that the initiation, extension, or renewal of an operation is necessary to avoid the loss of a significant investigative opportunity.

Before providing authorization in these situations, the SAC shall attempt to consult with the appropriate Federal prosecutor and with a designated Assistant Director.

(3) The power to provide emergency authorizations under subparagraph (2) may not be delegated pursuant to Section IV.B(3).

(4) In situations arising under subparagraph (2), a written application for approval must be submitted to FBIHQ within 48 hours after the operation has been initiated, extended, or renewed, together with the initial finding and a written description of the emergency situation. As soon as it is notified of an emergency authorization, FBIHQ shall notify the DOJ members of the Undercover Review Committee. If the subsequent written application for approval is denied, a full report of all activity undertaken during the course of the operation must be submitted to the Director, who shall inform the Deputy Attorney General.

(5) In online undercover operations, a SAC or his or her designee may authorize, in writing, continued online undercover contact for a period not to exceed 30 days if it is essential to continue online contact with a subject in order to either maintain credibility or avoid permanent loss of contact with a subject during the period of time in which an application for an online undercover operation is being prepared and submitted for approval. If the proposed undercover operation is one that must be approved by an Assistant Director under Section IV.C(2), the appropriate offices at FBIHQ must be notified promptly of the decision to grant this interim authority. Furthermore, a full report of all online activity occurring during this period must be submitted to the approving authority as soon as practicable. If approved, the undercover employee maintaining online contact during this period must:

(a) Maintain an accurate recording of all online communication;

(b) Avoid otherwise illegal activity;

(c) Maintain as limited an online profile as possible consistent with the need to accomplish the objectives stated above;

(d) Avoid physical contact with subjects;

(e) Take all necessary and reasonable actions during the interim period to protect potential victims and prevent serious criminal activity if online contact reveals a significant and imminent threat to third party individuals, commercial establishments, or government entities; and

(f) Cease undercover activities if, during the 30-day period, a determination is made to disapprove the undercover operation.

## V. PROTECTING INNOCENT PARTIES AGAINST ENTRAPMENT

### A. ENTRAPMENT

Entrapment must be scrupulously avoided. Entrapment occurs when the Government implants in the mind of a person who is not otherwise disposed to commit the offense the disposition to commit the offense and then induces the commission of that offense in order to prosecute.

### B. AUTHORIZATION REQUIREMENTS

In addition to the legal prohibition on entrapment, additional restrictions limit FBI undercover activity to ensure, insofar as it is possible, that entrapment issues do not adversely affect criminal prosecutions. As a result, no undercover activity involving an inducement to an individual to engage in crime shall be authorized unless the approving official is satisfied that –

(1) The illegal nature of the activity is reasonably clear to potential subjects; and

(2) The nature of any inducement offered is justifiable in view of the character of the illegal transaction in which the individual is invited to engage; and

(3) There is a reasonable expectation that offering the inducement will reveal illegal activity; and

(4) One of the two following limitations is met:

(i) There is reasonable indication that the subject is engaging, has engaged, or is likely to engage in the illegal activity proposed or in similar illegal conduct; or

(ii) The opportunity for illegal activity has been structured so that there is reason to believe that any persons drawn to the opportunity, or brought to it, are predisposed to engage in the contemplated illegal conduct.

## C. EXCEPTION

The alternative requirements of paragraph B(4), while not required by law, are imposed to ensure the Government does not offer inducements to crime to persons who are not predisposed to do so. These standards can be waived only by the Director upon a written finding that the activities are necessary to protect life or prevent other serious harm.

# VI. MONITORING AND CONTROL OF UNDERCOVER OPERATIONS

## A. PREPARATION OF UNDERCOVER EMPLOYEES, INFORMANTS, AND COOPERATING WITNESSES

(1) Prior to the investigation, the SAC or a designated Supervisory Special Agent shall review with each undercover employee the conduct that the undercover employee is expected to undertake and conduct that may be necessary during the investigation. The SAC or Agent shall discuss with each undercover employee any of the sensitive or fiscal circumstances specified in Section IV.C(1) or (2) that are reasonably likely to occur.

(2) Each undercover employee shall be instructed that he or she shall not participate in any act of violence; initiate or instigate any plan to commit criminal acts; use unlawful investigative techniques to obtain information or evidence; or engage in any conduct that would violate restrictions on investigative techniques or FBI conduct contained in the Attorney General's Guidelines or departmental policy; and that, except in an emergency situation as set out in Section IV.H(5)(d), he or she shall not participate in any illegal activity for which authorization has not been obtained under these Guidelines. The undercover employee shall be instructed in the law of entrapment. When an undercover employee learns that persons under investigation intend to commit a violent crime, he or she shall try to discourage the violence.

## B. REVIEW OF CONDUCT

From time to time, during the course of the undercover operation, the SAC shall review the conduct of the undercover employee(s) and others participating in the undercover operation, including any proposed or reasonably foreseeable conduct for the remainder of the investigation. Any findings of impermissible conduct shall be discussed with the individual and promptly reported to the designated Assistant Director and the members of the Undercover Review Committee, and a determination shall be made as to whether the individual should continue his or her participation in the investigation.

## C. CONTINUING CONSULTATION WITH THE APPROPRIATE FEDERAL PROSECUTOR

Upon initiating and throughout the course of any undercover operation, the SAC or a designated Supervisory Special Agent shall consult on a continuing basis with the appropriate

Federal prosecutor, particularly with respect to the propriety of the operation and the legal sufficiency and quality of evidence that is being produced by the activity.

## D. SERIOUS LEGAL, ETHICAL, PROSECUTIVE OR DEPARTMENTAL POLICY QUESTIONS, AND PREVIOUSLY UNFORESEEN SENSITIVE CIRCUMSTANCES

(1) The SAC shall consult with the chairman of the Criminal Undercover Operations Review Committee, FBIHQ whenever a serious legal, ethical, prosecutive, or departmental policy question arises in any undercover operation or if sensitive circumstances occur that were not anticipated. The FBI shall consult with the United States Attorney, or Assistant Attorney General, or their representative, and with DOJ members of the Undercover Review Committee on whether to modify, suspend, or terminate the investigation related to such issues.

(2) When unforeseen sensitive circumstances arise, the SAC shall submit a written application to FBIHQ for authorization of an undercover operation previously approved at the field office level, or amend the existing application to FBIHQ pursuant to Section IV.F.

## E. ANNUAL REPORT OF THE UNDERCOVER REVIEW COMMITTEE

(1) The Undercover Review Committee shall retain a file of all applications for approval of undercover operations submitted to it, together with a written record of the Committee's action on the application and any ultimate disposition by the approving official. The FBI shall also prepare a short summary of each undercover operation recommended for approval by the Committee. These records and summaries shall be available for inspection by a designee of the Deputy Attorney General and of the Assistant Attorney General in charge of the Criminal Division.

(2) On an annual basis, the Committee shall submit to the Director, the Attorney General, the Deputy Attorney General, and the Assistant Attorney General in charge of the Criminal Division a written report summarizing:

(a) the types of undercover operations approved and disapproved together with the reasons for disapproval;

(b) the major issues addressed by the Committee in reviewing applications and how they were resolved; and

(c) any significant modifications to the operations recommended by the Committee.

## F. DEPOSIT OF PROCEEDS; LIQUIDATION OF PROPRIETARIES

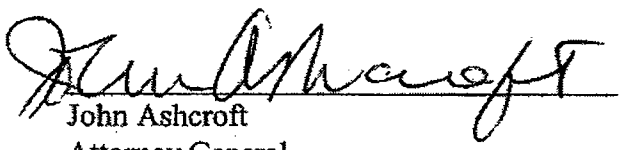
As soon as the proceeds from any undercover operation are no longer necessary for the conduct of the activity, the remaining proceeds shall be deposited in the Treasury of the United States as miscellaneous receipts.

Whenever a proprietary with a net value over the amount specified by the Department of Justice Appropriation Authorization Act or other applicable laws is to be liquidated, sold, or otherwise disposed of, the FBI shall report the circumstances to the Attorney General and the Comptroller General. The proceeds of the liquidation, sale, or the disposition, after obligations are met, shall be deposited in the Treasury of the United States as miscellaneous receipts.

## VII. RESERVATION

These Guidelines are set forth solely for the purpose of internal DOJ guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable by law by any party in any matter, civil or criminal, nor do they place any limitations on otherwise lawful investigative or litigative prerogatives of the Department of Justice.

Date: May 30, 2002



John Ashcroft
Attorney General

**BLANK PAGE**

# 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

## 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;

(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.

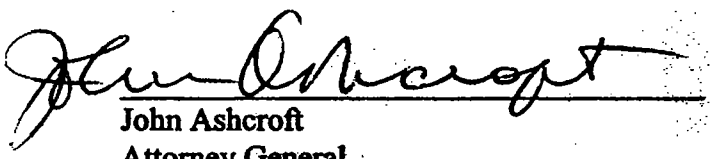
## VII. RESERVATION

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

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

May 30, 2002

MEMORANDUM FOR THE HEADS AND INSPECTORS GENERAL
OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: THE ATTORNEY GENERAL

SUBJECT: Procedures for Lawful, Warrantless Monitoring of Verbal Communications

By Memorandum dated October 16, 1972, the Attorney General directed all federal departments and agencies to obtain Department of Justice authorization before intercepting verbal communications without the consent of all parties to the communication. This directive was clarified and continued in force by the Attorney General's Memorandum of September 22, 1980, to Heads and Inspectors General of Executive Departments and Agencies. It was then superseded, with new authorization procedures and relevant rules and guidelines, including limitations on the types of investigations requiring prior written approval by the Department of Justice, in the Attorney General's Memorandum of November 7, 1983.[1]

The Attorney General's Memorandum of January 20, 1998, superseded the aforementioned directives. It continued most of the authorization procedures established in the November 7, 1983, Memorandum, but reduced the sensitive circumstances under which prior written approval of senior officials of the Department of Justice's Criminal Division is required. At the same time, it continued to require oral authorization from Department of Justice attorneys, ordinarily local Assistant United States Attorneys, before the initiation of the use of consensual monitoring in all investigations not requiring prior written approval. In addition, that Memorandum reduced and eventually eliminated the reporting requirement imposed on departments and agencies. These changes reflected the results of the exercise of the Department's review function over many years, which showed that the departments and agencies had uniformly been applying the required procedures with great care, consistency, and good judgment, and that the number of requests for consensual monitoring that were not approved had been negligible.

---

[1]As in all of the prior memoranda except for the one dated October 16, 1972, this memorandum only applies to the consensual monitoring of oral, nonwire communications, as discussed below. "Verbal" communications will hereinafter be referred to as oral.

This Memorandum updates and in some limited respects modifies the Memorandum of January 20, 1998. The changes are as follows:

First, Parts III.A.(8) and V. of the January 20, 1998, Memorandum required concurrence or authorization for consensual monitoring by the United States Attorney, an Assistant United States Attorney, or the previously designated Department of Justice attorney responsible for a particular investigation (for short, a "trial attorney"). This Memorandum provides instead that a trial attorney must advise that the monitoring is legal and appropriate. This continues to limit monitoring to cases in which an appropriate attorney agrees to the monitoring, but makes it clear that this function does not establish a supervisory role or require any involvement by the attorney in the conduct of the monitoring. In addition, for cases in which this advice cannot be obtained from a trial attorney for reasons unrelated to the legality or propriety of the monitoring, this Memorandum provides a fallback procedure to obtain the required advice from a designated attorney of the Criminal Division of the Department of Justice. Where there is an issue as to whether providing the advice would be consistent with applicable attorney conduct rules, the trial attorney or the designated Criminal Division attorney should consult with the Department's Professional Responsibility Advisory Office.

Second, Part V. of the Memorandum of January 20, 1998, required that an agency head or his or her designee give oral authorization for consensual monitoring, and stated that "[a]ny designee should be a high-ranking supervisory official at headquarters level." This rule was qualified by Attorney General Order No. 1623-92 of August 31, 1992, which, in relation to the Federal Bureau of Investigation (FBI), authorized delegation of this approval function to Special Agents in Charge. Experience has shown that the requirement of Special Agent in Charge approval can result in a loss of investigative opportunities because of an overly long approval process, and indicates that allowing approval by Assistant Special Agents in Charge would facilitate FBI investigative operations. Assistant Special Agents in Charge are management personnel to whom a variety of supervisory and oversight responsibilities are routinely given; generally, they are directly involved and familiar with the circumstances relating to the propriety of proposed uses of the consensual monitoring technique. Part V. is accordingly revised in this Memorandum to provide that the FBI Director's designees for purposes of oral authorization of consensual monitoring may include both Special Agents in Charge and Assistant Special Agents in Charge. This supersedes Attorney General Order No. 1623-92, which did not allow delegation of this function below the level of Special Agent in Charge.

Third, this Memorandum omits as obsolete Part VI. of the Memorandum of January 20, 1998. Part VI. imposed a reporting requirement by agencies concerning consensual monitoring but rescinded that reporting requirement after one year.

The Fourth Amendment to the United States Constitution, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended (18 U.S.C. §2510, et seq.), and the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. §1801, et seq.) permit government agents,

acting with the consent of a party to a communication, to engage in warrantless monitoring of wire (telephone) communications and oral, nonwire communications. See United States v. White, 401 U.S. 745 (1971); United States v. Caceres, 440 U.S. 741 (1979). Similarly, the Constitution and federal statutes permit federal agents to engage in warrantless monitoring of oral, nonwire communications when the communicating parties have no justifiable expectation of privacy.[2] Because such monitoring techniques are particularly effective and reliable, the Department of Justice encourages their use by federal agents for the purpose of gathering evidence of violations of federal law, protecting informants or undercover law enforcement agents, or fulfilling other, similarly compelling needs. While these techniques are lawful and helpful, their use in investigations is frequently sensitive, so they must remain the subject of careful, self-regulation by the agencies employing them.

The sources of authority for this Memorandum are Executive Order No. 11396 ("Providing for the Coordination by the Attorney General of Federal Law Enforcement and Crime Prevention Programs"); Presidential Memorandum ("Federal Law Enforcement Coordination, Policy and Priorities") of September 11, 1979; Presidential Memorandum (untitled) of June 30, 1965, on, inter alia, the utilization of mechanical or electronic devices to overhear nontelephone conversations; the Paperwork Reduction Act of 1980 and the Paperwork Reduction Reauthorization Act of 1986, as amended; and the inherent authority of the Attorney General as the chief law enforcement officer of the United States.

## I. DEFINITIONS

As used in this Memorandum, the term "agency" means all of the Executive Branch departments and agencies, and specifically includes United States Attorneys' Offices which utilize their own investigators, and the Offices of the Inspectors General.

As used in this Memorandum, the terms "interception" and "monitoring" mean the aural acquisition of oral communications by use of an electronic, mechanical, or other device. Cf. 18 U.S.C. § 2510(4).

As used in this Memorandum, the term "public official" means an official of any public entity of government, including special districts, as well as all federal, state, county, and municipal governmental units.

---

[2]As a general rule, nonconsensual interceptions of wire communications violate 18 U.S.C. § 2511 regardless of the communicating parties' expectation of privacy, unless the interceptor complies with the court-authorization procedures of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. § 2510, et seq.) or with the provisions of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801 et seq.).

## II. NEED FOR WRITTEN AUTHORIZATION

### A. Investigations Where Written Department of Justice Approval is Required

A request for authorization to monitor an oral communication without the consent of all parties to the communication must be approved in writing by the Director or Associate Director of the Office of Enforcement Operations, Criminal Division, U.S. Department of Justice, when it is known that:

(1) the monitoring relates to an investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years;

(2) the monitoring relates to an investigation of the Governor, Lieutenant Governor, or Attorney General of any State or Territory, or a judge or justice of the highest court of any State or Territory, and the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his or her official duties;

(3) any party to the communication is a member of the diplomatic corps of a foreign country;

(4) any party to the communication is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers;

(5) the consenting or nonconsenting person is in the custody of the Bureau of Prisons or the United States Marshals Service; or

(6) the Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, or the United States Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent before conducting consensual monitoring in a specific investigation.

In all other cases, approval of consensual monitoring will be in accordance with the procedures set forth in part V. below.

B. Monitoring Not Within Scope of Memorandum

Even if the interception falls within one of the six categories above, the procedures and rules in this Memorandum do not apply to:

(1) extraterritorial interceptions;

(2) foreign intelligence interceptions, including interceptions pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801, et seq.);

(3) interceptions pursuant to the court-authorization procedures of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended (18 U.S.C. § 2510, et seq.);

(4) routine Bureau of Prisons monitoring of oral communications that are not attended by a justifiable expectation of privacy;

(5) interceptions of radio communications; and

(6) interceptions of telephone communications.

III. AUTHORIZATION PROCEDURES AND RULES

A. Required Information

The following information must be set forth in any request to monitor an oral communication pursuant to part II.A.:

(1) Reasons for the Monitoring. The request must contain a reasonably detailed statement of the background and need for the monitoring.

(2) Offense. If the monitoring is for investigative purposes, the request must include a citation to the principal criminal statute involved.

(3) Danger. If the monitoring is intended to provide protection to the consenting party, the request must explain the nature of the danger to the consenting party.

(4) Location of Devices. The request must state where the monitoring device will be hidden: on the person, in personal effects, or in a fixed location.

(5) Location of Monitoring. The request must specify the location and primary judicial district where the monitoring will take place. A monitoring authorization is not restricted to the original district. However, if the location of monitoring changes, notice should be promptly given to the approving official. The record maintained on the request should reflect the location change.

(6) Time. The request must state the length of time needed for the monitoring. Initially, an authorization may be granted for up to 90 days from the day the monitoring is scheduled to begin. If there is the need for continued monitoring, extensions for additional periods of up to 90 days may be granted. In special cases (e.g., "fencing" operations run by law enforcement agents or long-term investigations that are closely supervised by the Department's Criminal Division) authorization for up to 180 days may be granted with similar extensions.

(7) Names. The request must give the names of persons, if known, whose communications the department or agency expects to monitor and the relation of such persons to the matter under investigation or to the need for the monitoring.

(8) Attorney Advice. The request must state that the facts of the surveillance have been discussed with the United States Attorney, an Assistant United States Attorney, or the previously designated Department of Justice attorney responsible for a particular investigation, and that such attorney advises that the use of consensual monitoring is appropriate under this Memorandum (including the date of such advice). The attorney must also advise that the use of consensual monitoring under the facts of the investigation does not raise the issue of entrapment. Such statements may be made orally. If the attorneys described above cannot provide the advice for reasons unrelated to the legality or propriety of the consensual monitoring, the advice must be sought and obtained from an attorney of the Criminal Division of the Department of Justice designated by the Assistant Attorney General in charge of that Division. Before providing such advice, a designated Criminal Division Attorney shall notify the appropriate United States Attorney or other attorney who would otherwise be authorized to provide the required advice under this paragraph.

(9) Renewals. A request for renewal authority to monitor oral communications must contain all the information required for an initial request. The renewal request must also refer to all previous authorizations and explain why an additional authorization is needed, as well as provide

an updated statement that the attorney advice required under paragraph (8) has been obtained in connection with the proposed renewal.

B. Oral Requests

Unless a request is of an emergency nature, it must be in written form and contain all of the information set forth above. Emergency requests in cases in which written Department of Justice approval is required may be made by telephone to the Director or an Associate Director of the Criminal Division's Office of Enforcement Operations, or to the Assistant Attorney General, the Acting Assistant Attorney General, or a Deputy Assistant Attorney General for the Criminal Division, and should later be reduced to writing and submitted to the appropriate headquarters official as soon as practicable after authorization has been obtained. An appropriate headquarters filing system is to be maintained for consensual monitoring requests that have been received and approved in this manner. Oral requests must include all the information required for written requests as set forth above.

C. Authorization

Authority to engage in consensual monitoring in situations set forth in part II.A. of this Memorandum may be given by the Attorney General, the Deputy Attorney General, the Associate Attorney General, the Assistant Attorney General or Acting Assistant Attorney General in charge of the Criminal Division, a Deputy Assistant Attorney General in the Criminal Division, or the Director or an Associate Director of the Criminal Division's Office of Enforcement Operations. Requests for authorization will normally be submitted by the headquarters of the department or agency requesting the consensual monitoring to the Office of Enforcement Operations for review.

D. Emergency Monitoring

If an emergency situation requires consensual monitoring at a time when one of the individuals identified in part III.B. above cannot be reached, the authorization may be given by the head of the responsible department or agency, or his or her designee. Such department or agency must then notify the Office of Enforcement Operations as soon as practicable after the emergency monitoring is authorized, but not later than three working days after the emergency authorization.

The notification shall explain the emergency and shall contain all other items required for a nonemergency request for authorization set forth in part III.A. above.

## IV. SPECIAL LIMITATIONS

When a communicating party consents to the monitoring of his or her oral communications, the monitoring device may be concealed on his or her person, in personal effects, or in a fixed location. Each department and agency engaging in such consensual monitoring must ensure that the consenting party will be present at all times when the device is operating. In addition, each department and agency must ensure: (1) that no agent or person cooperating with the department or agency trespasses while installing a device in a fixed location, unless that agent or person is acting pursuant to a court order that authorizes the entry and/or trespass, and (2) that as long as the device is installed in the fixed location, the premises remain under the control of the government or of the consenting party. See United States v. Yonn, 702 F.2d 1341, 1347 (11th Cir.), cert. denied, 464 U.S. 917 (1983) (rejecting the First Circuit's holding in United States v. Padilla, 520 F.2d 526 (1st Cir. 1975), and approving use of fixed monitoring devices that are activated only when the consenting party is present). But see United States v. Shabazz, 883 F. Supp. 422 (D. Minn. 1995).

Outside the scope of this Memorandum are interceptions of oral, nonwire communications when no party to the communication has consented. To be lawful, such interceptions generally may take place only when no party to the communication has a justifiable expectation of privacy,[3] or when authorization to intercept such communications has been obtained pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. § 2510, et seq.) or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801 et seq.). Each department or agency must ensure that no communication of any party who has a justifiable expectation of privacy is intercepted unless proper authorization has been obtained.

## V. PROCEDURES FOR CONSENSUAL MONITORING WHERE NO WRITTEN APPROVAL IS REQUIRED

Prior to receiving approval for consensual monitoring from the head of the department or agency or his or her designee, a representative of the department or agency must obtain advice that the consensual monitoring is both legal and appropriate from the United States Attorney, an Assistant United States Attorney, or the Department of Justice attorney responsible for a particular investigation. The advice may be obtained orally from the attorney. If the attorneys described above cannot provide this advice for reasons unrelated to the legality or propriety of the consensual monitoring, the advice must be

---

[3]For example, burglars, while committing a burglary, have no justifiable expectation of privacy. Cf. United States v. Pui Kan Lam, 483 F.2d 1202 (2d. Cir. 1973), cert. denied, 415 U.S. 984 (1974).

sought and obtained from an attorney of the Criminal Division of the Department of Justice designated by the Assistant Attorney General in charge of that Division. Before providing such advice, a designated Criminal Division Attorney shall notify the appropriate United States Attorney or other attorney who would otherwise be authorized to provide the required advice under this paragraph.

Even in cases in which no written authorization is required because they do not involve the sensitive circumstances discussed above, each agency must continue to maintain internal procedures for supervising, monitoring, and approving all consensual monitoring of oral communications. Approval for consensual monitoring must come from the head of the agency or his or her designee. Any designee should be a high-ranking supervisory official at headquarters level, but in the case of the FBI may be a Special Agent in Charge or Assistant Special Agent in Charge.

Similarly, each department or agency shall establish procedures for emergency authorizations in cases involving non-sensitive circumstances similar to those that apply with regard to cases that involve the sensitive circumstances described in part III.D., including obtaining follow-up oral advice of an appropriate attorney as set forth above concerning the legality and propriety of the consensual monitoring.

Records are to be maintained by the involved departments or agencies for each consensual monitoring that they have conducted. These records are to include the information set forth in part III.A. above.

## VI. GENERAL LIMITATIONS

This Memorandum relates solely to the subject of consensual monitoring of oral communications except where otherwise indicated. This Memorandum does not alter or supersede any current policies or directives relating to the subject of obtaining necessary approval for engaging in nonconsensual electronic surveillance or any other form of nonconsensual interception.

# APPENDIX C

# TABLE OF REVISIONS TO THE ATTORNEY GENERAL'S INVESTIGATIVE GUIDELINES OF MAY 30, 2002

| General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations | | |
|---|---|---|
| **Section** | **Previous Version 03/21/1989** | **Current Version 05/30/2002** |
| **Preamble** | | |
| | "As the primary criminal investigative agency in the federal government, the FBI has the authority and responsibility to investigate all criminal violations of federal law not exclusively assigned to another federal agency. The FBI thus plays a central role in national law enforcement and in the proper administration of justice in the United States."<br><br>"Investigations by the FBI are premised upon the important duty of government to protect the public against general crimes, against organized criminal activity, and against those who would engage in political or racial terrorism or would destroy our constitutional system through criminal violence." | Adds text addressing terrorist acts:<br><br>"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."<br><br>"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." |
| **Introduction** | | |
| Checking of Leads and Preliminary Inquiries | No Corresponding Text | Adds text describing progression through levels of investigative activity:<br><br>"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." [Introduction A.] |

| General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations | | |
|---|---|---|
| **Section** | **Previous Version 03/21/1989** | **Current Version 05/30/2002** |
| Checking of Leads and Preliminary Inquiries | No Corresponding Text | Adds text emphasizing role of preliminary inquiries in cases involving weapons of mass destruction:<br><br>"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." [Introduction A.]<br><br>"[W]here 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." [Introduction A.] |
| **Part I: General Principles** | | |
| | "All preliminary inquiries shall be conducted pursuant to the General Crimes Guidelines. There is no separate provision for a preliminary inquiry under the Criminal Intelligence Guidelines." [I.] | Authorizes preliminary inquiries to determine whether to commence Racketeering Enterprise or Terrorism Enterprise Investigations:<br><br>"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." [I.] |

| General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations | | |
|---|---|---|
| **Section** | **Previous Version 03/21/1989** | **Current Version 05/30/2002** |
| **Part II: General Crimes Investigations** | | |
| Preliminary Inquiries | "Inquiries shall be completed within 90 days after initiation of the first investigative step. [A]n extension of time in an inquiry for succeeding 30-day periods may be granted . . ." [II.B.3.] | Lengthens period of initial inquiry and extensions of time to:<br>180 days for initial inquiry<br>90 days for extensions [II.B.3.] |
| | "An extension of time in an inquiry . . . may be granted by FBI Headquarters upon receipt of written request and statement of reasons why further investigative steps are warranted when there is no 'reasonable indication' of criminal activity." [II.B.3.] | - Delegates to field offices authority to grant first two extensions<br>- All further extensions are granted only by FBIHQ. [II.B.3.] |
| | "Whether an intrusive technique should be used in an inquiry depends on the seriousness of the possible crime and the strength of the information indicating the possible existence of the crime." [II.B.4.] | Adds considerations in determining investigative techniques:<br><br>"The FBI should not hesitate to use any lawful techniques . . . 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." [II.B.4.] |
| | "Some of the factors to be considered in judging intrusiveness are adverse consequences to an individual's privacy interests and avoidable damage to his reputation. [I]t is recognized that choice of technique is a matter of judgment." [II.B.4.] | Adds considerations in determining investigative techniques:<br><br>"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." [II.B.4.] |
| | Prohibited the use of mail covers during preliminary inquiries. [II.B.5.] | Authorizes the use of mail covers in preliminary inquiries. [II.B.5.] |
| | "Where a technique is highly intrusive, a supervisory agent shall approve its use in the inquiry stage only in compelling circumstances and when other investigative means are not likely to be successful." [II.B.6.] | Eliminates requirement for supervisory approval of highly intrusive investigative techniques. [II.B.6] |

| General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations | | |
|---|---|---|
| **Section** | **Previous Version 03/21/1989** | **Current Version 05/30/2002** |
| **Part III: Criminal Intelligence Investigations** | | |
| Racketeering Enterprise Investigations | "The FBI has authority to conduct investigations of racketeering enterprises whose activities involve violence, extortion, narcotics, or systematic public corruption. A racketeering enterprise not engaged in such activities may be investigated . . . only upon a written determination by the Director, concurred in by the Attorney General, that such investigation is justified by exceptional circumstances." [III.A.2.a.] | Eliminates enumerated predicate crimes and substitutes "pattern of racketeering activity" as defined in the RICO statute. [III.A.2.a.] |
| | "A racketeering enterprise investigation may be initiated when facts or circumstances reasonably indicate that two or more persons are engaged in a continuing course of conduct for the purpose of obtaining monetary or commercial gains or profits wholly or in part through racketeering activity." [III.A.2.b.] | Defines facts or circumstances for initiation of racketeering enterprise investigation as those contained in the RICO statute:<br><br>"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)." [III.A.2.a.] |
| | No Corresponding Text | Adds circumstances under which racketeering activity is treated as a terrorism enterprise investigation:<br><br>"[i]f 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." [III.A.2.a.] |
| | "A racketeering enterprise investigation may be authorized by the Director or designated Assistant Director upon a written recommendation . . ." [III.A.5.a.] | Delegates to field offices authority to initiate racketeering enterprise investigation:<br><br>"A racketeering enterprise investigation may be authorized by the Special Agent in Charge, with notification to FBIHQ upon a written recommendation. . ." [III.A.5.a.] |

| General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations | | |
|---|---|---|
| **Section** | **Previous Version 03/21/1989** | **Current Version 05/30/2002** |
| Racketeering Enterprise Investigations | "The FBI shall notify the Attorney General or his designee of the opening of the investigation." [III.A.5.a.] | Requires notification of the DOJ Organized Crime and Racketeering Section, which in turn, notifies the Attorney General:<br><br>"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." [III.A.5.b.] |
| | "[t]he Attorney General may, as he deems necessary, request the FBI to provide a report on the status of the investigation." [III.A.5.a.] | Delegates to Chief of the DOJ Organized Crime and Racketeering Section authority to request FBI reports:<br><br>"[t]he 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." [III.A.5b.] |
| | "A racketeering enterprise investigation may be initially authorized for a period of up to 180 days. An investigation may be continued upon renewed authorization for additional periods each not to exceed 180 days." [III.A.5.b.] | Lengthens period for initial authorizations and renewals:<br><br>"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." [III.A.5.c.] |
| | "Renewal authorization shall be obtained from the Director or designated Assistant Director." [III.A.5.b.] | Delegates to field offices authority to renew racketeering enterprise investigations and requires notification to DOJ:<br><br>"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." [III.A.5.c.] |

| General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations | | |
|---|---|---|
| **Section** | **Previous Version 03/21/1989** | **Current Version 05/30/2002** |
| Racketeering Enterprise Investigations | "Investigations shall be reviewed by the Director or designated senior Headquarters official on or before the expiration of the period for which the investigation and each renewal thereof is authorized." [III.A.5.c.] | Delegates to field offices authority to review racketeering enterprise investigations prior to renewal:<br><br>"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." [III.A.5.d.] |
| | "A racketeering enterprise investigation may be authorized by the Director or designated Assistant Director upon a written recommendation setting forth the facts and circumstances reasonably indicating the existence of a racketeering enterprise whose activities involve violence, extortion, narcotics, or systematic public corruption. In such cases the FBI shall notify the Attorney General or his designee of the opening of the investigation. An investigation of a racketeering enterprise not involved in these activities may be authorized only by the Director upon his written determination, concurred in by the Attorney General, that such investigation is warranted by exceptional circumstances. . . . Renewal authorization shall be obtained from the Director or designated Assistant Director. The concurrence of the Attorney General must also be obtained if his concurrence was initially required to authorize the investigation." [III.A.5.a-b] | Expands authority to initiate, renew, review, and reopen racketeering enterprise investigations:<br><br>"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." [III.A.5.f.] |

| General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations | | |
|---|---|---|
| **Section** | **Previous Version 03/21/1989** | **Current Version 05/30/2002** |
| Terrorism Enterprise Investigations | "A domestic security/terrorism investigation may be initiated when the facts or circumstances reasonably indicate that two or more persons are engaged in an enterprise for the purpose of furthering political or social goals wholly or in part through activities that involve force or violence and a violation of the criminal laws of the United States." [III.B.1.a.] | Adds additional bases for initiating terrorism enterprise investigations:<br><br>"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)." [III.B.1.a.] |
| | "A domestic security/terrorism investigation may be authorized by the Director or designated Assistant upon a written recommendation setting forth the facts or circumstances reasonably indicating the existence of an enterprise as described in this subsection. In such cases, the FBI shall notify the Office of Intelligence Policy and Review of the opening of the investigation." [III.B.4.a.] | Delegates to field offices authority to initiate terrorism enterprise investigations and changes notification requirements to the DOJ:<br><br>"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." [III.B.4.a.] |

| General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations | | |
|---|---|---|
| **Section** | **Previous Version 03/21/1989** | **Current Version 05/30/2002** |
| Terrorism Enterprise Investigations | "In all investigations the Attorney General may, as he deems necessary, request the FBI to provide a report on the status of the investigation." [III.B.4.a.] | Delegates to the Chief of DOJ Terrorism and Violent Crime Section authority to request FBI reports:<br><br>"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." [III.B.4.a.] |
| | "A domestic security/terrorism investigation may be initially authorized for a period of up to 180 days. An investigation may be continued upon renewed authorization for additional periods each not to exceed 180 days." [III.B.4.b.] | Lengthens period of initial authorization and renewals:<br><br>"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." [III.B.4.b.] |
| | "Renewal authorization shall be obtained from the Director or designated Assistant Director." [III.B.4.b.] | Delegates to field offices authority to renew terrorism enterprise investigations and requires notification to DOJ:<br><br>"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." [III.B.4.b.] |
| | "Investigations shall be reviewed by the Director or designated Senior Headquarters official on or before the expiration period for which the investigation and each renewal thereof is authorized." [III.B.4.c.] | Delegates to field offices authority to review terrorism enterprise investigations:<br><br>"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." [III.B.4.c.] |

| General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations | | |
|---|---|---|
| **Section** | **Previous Version 03/21/1989** | **Current Version 05/30/2002** |
| Terrorism Enterprise Investigations | "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, nor is there any immediate threat of harm – yet the composition, goals and prior history of the group suggests the need for continuing federal interest. Under those circumstances, the investigation may be continued but reasonable efforts should be made to limit the coverage to information which might indicate a change in the status or criminal objectives of the enterprise." [III.B.4.d.] | Eliminates requirement to limit scope of temporarily inactive investigations:<br><br>"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." [III.B.4.c.] |
| | "A domestic security/terrorism investigation may be authorized by the Director or designated Assistant Director upon a written recommendation setting forth the facts or circumstances reasonably indicating the existence of an enterprise as described in this subsection. . . . Renewal authorization shall be obtained from the Director or designated Assistant Director. Investigations shall be reviewed by the Director or designated Senior Headquarters official on or before the expiration period for which the investigation and each renewal thereof is authorized." [III.B.4.a-c] | Expands authority to initiate, renew, review, and reopen terrorism enterprise investigations:<br><br>"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." [III.B.4.e.] |
| **Part IV: Investigative Techniques** | | |
| | "Some of the factors to be considered in judging intrusiveness are adverse consequences to an individual's privacy interest and avoidable damage to his reputation. [I]t is recognized that choice of technique is a matter of judgment." [IV.A.] | Adds considerations in determining investigative techniques:<br><br>"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." [IV.A.] |

| General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations | | |
|---|---|---|
| **Section** | **Previous Version 03/21/1989** | **Current Version 05/30/2002** |
| | "Whether a highly intrusive technique should be used depends on the seriousness of the crime and the strength of the information indicating the existence of the crime." [IV.A.] | "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." [IV.A.] |
| | "All requirements for use of a technique set by statute, Department regulations and policies, and Attorney General Guidelines must be complied with." The listed investigative techniques are subject to the noted restrictions. [IV.B.] | Adds "classified investigative technologies" to list of investigative techniques. [IV.B.9.] |
| | "Undisclosed participation in the activities of an organization by an undercover employee or cooperating private individual in a manner that may influence the exercise of rights protected by the First Amendment must be approved by FBIHQ, with notification to Department of Justice." [IV.B.3.] | Eliminates FBIHQ and DOJ approval requirements and substitutes compliance with the Attorney General Guidelines:<br><br>"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" [IV.B.3.] |
| | "For consensual monitoring of telephone conversations, advance authorization must be obtained from the SAC and the appropriate U.S. Attorney, except in exigent circumstances." [IV.B.7.] | Expands approval authority in field offices and DOJ:<br><br>"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" [IV.B.7.] |

| General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations | | |
|---|---|---|
| **Section** | **Previous Version 03/21/1989** | **Current Version 05/30/2002** |
| | No Corresponding Text | Adds consultation requirement with the Professional Responsibility Advisory Office:<br><br>"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." [IV.B.10.] |
| **Part V: Dissemination and Maintenance of Information** | | |
| | "The FBI may disseminate information during investigations conducted pursuant to these guidelines to another Federal agency or to a State or local criminal justice agency when such information: A. falls within the investigative or protective jurisdiction or litigative responsibility of the agency; B. may assist in preventing a crime or the use of violence or any other conduct dangerous to human life; C. is required to be furnished to another Federal agency by Executive Order 10450, as amended, dated April 27, 1953, or a successor Order; D. is required to be disseminated by statute, interagency agreement approved by the Attorney General, or Presidential Directive; and to other persons and agencies as permitted by Section 552 and 552a of Title V, U.S.C. " [V.A.] | Authorizes dissemination of information during checking of leads and preliminary inquiries and clarifies practices with respect to the DOJ:<br><br>"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: A. falls within the investigative or protective jurisdiction or litigative responsibility of the agency; B. may assist in preventing a crime or the use of violence or any other conduct dangerous to human life; C. is required to be furnished to another Federal agency by Executive Order 10450, as amended, dated April 27, 1953, or a successor Order; D. is required to be disseminated by statute, interagency agreement approved by the Attorney General, or Presidential Directive; and to other persons and agencies as permitted by Section 552 and 552a of Title V, U.S.C. " [V.A.] |

| General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations | | |
|---|---|---|
| **Section** | **Previous Version 03/21/1989** | **Current Version 05/30/2002** |
| | No Corresponding Text | Requires maintenance of database on preliminary inquiries and investigations:<br><br>"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." [V.B.] |
| **Part VI: Counterterrorism Activities and Other Authorizations** | | |
| Counter-terrorism Activities | No Corresponding Text | Authorizes information systems:<br>-FBI may operate and participate in identification, tracking, and information systems for purposes of detecting, prosecuting, or preventing terrorism.<br>-System information may come from sources permitted by law, prior or ongoing investigations, government sources, public sources, and voluntary private sources.<br>-Systems operated by the FBI must be reviewed periodically for compliance with applicable statutes, rules, regulations, and Guidelines. [VI.A.1.] |
| | No Corresponding Text | Authorizes the visiting of public places and events:<br>-FBI may visit any place and attend any event that is open to the public, for purposes of detecting or preventing terrorism.<br>- Information may not be retained from such visits unless it relates to potential criminal or terrorist activity. [VI.A.2.] |

| General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations | | |
|---|---|---|
| **Section** | **Previous Version 03/21/1989** | **Current Version 05/30/2002** |
| Other Authorizations | No Corresponding Text | Authorizes online general topical research:<br>-FBI may search and access online sites and forums on subject areas to facilitate or support investigative responsibilities.<br>-Prohibits online searches on individual names or identifiers except where incidental to topical research. [VI.B.1.] |
| | No Corresponding Text | Authorizes the FBI to conduct online searches and access online sites and forums for the purposes of detecting or preventing terrorism or other criminal activities. [VI.B.2.] |
| | No Corresponding Text | Authorizes the FBI to prepare general reports and assessments on terrorism or other criminal activities for purposes of strategic planning or investigative support. [VI.B.3.] |
| Protecting Privacy and Other Limitations | No Corresponding Text | Prohibits FBI pursuant to exercise of law enforcement activities authorized by Part VI from maintaining files on individuals solely for the purpose of monitoring First Amendment activities or other rights protected by the Constitution. [VI.C.1.] |
| | No Corresponding Text | Requires all law enforcement activities authorized by Part VI to have a valid law enforcement purpose. [VI.C.1.] |
| | No Corresponding Text | Summarizes provisions of the Privacy Act and directs questions concerning its applicability to the FBI Office of General Counsel or the Office of Information and Privacy |

[BLANK PAGE]

| Consensual Monitoring | | |
|---|---|---|
| **Section** | **Previous Version 01/20/1998** | **Current Version 05/30/2002** |
| **Part III. Authorization Procedures and Rules** | | |
| Required Information | U.S. Attorney, Assistant U.S. Attorney or other designated DOJ attorney must concur that the use of consensual monitoring is appropriate and does not raise the issue of entrapment. [III.A.8] | Changes "concur" to "advise;" provides that designated Criminal Division attorney must advise if trial attorney cannot provide advice for reasons unrelated to the legality or propriety of the consensual monitoring. [III.A.8] |
| | Updated statement of attorney concurrence is required. [III.A.9] | Requires updated statement of attorney advice. [III.A.9] |
| **Part V. Procedures for Consensual Monitoring Where No Written Approval Is Required** | | |
| | Approval required from U.S. Attorney, Assistant U.S. Attorney, or DOJ attorney responsible for investigation. Approval may be oral, and attorney must concur as to both legality and propriety of consensual monitoring. [V] | Changes "approval" to "advice"; provides that designated Criminal Division attorney must advise if trial attorney cannot provide advice for reasons unrelated to the legality or propriety of the consensual monitoring. [V] |
| | Approval for consensual monitoring must come from the head of the agency or his or her designee. Any designee should be a high-ranking supervisory official at headquarters level. [V] | Expands approval authority for FBI designee to include SAC or ASAC. [V] |
| | Attorney authorization required. [V] | Changes "authorization" to "advice." [V] |

[BLANK PAGE]

| Confidential Informants | | |
|---|---|---|
| **Section** | **Previous Version 01/08/2001** | **Current Version 05/30/2002** |
| **Part II. Registering a Confidential Informant** | | |
| Instructions | Agents required reading to all CIs verbatim the general instructions applicable to all CIs. | Agents no longer required to read general instructions verbatim to CIs but must review written instructions with CIs at registration and thereafter as required, but at least annually. [II.C] |
| | Agents required to read the following instructions verbatim to all CIs:<br><br>The United States Government will strive to protect your identity, but cannot promise or guarantee either that you identity will not be divulged as a result of legal or other compelling considerations, or that you will not be called to testify in a proceeding as a witness." [II.C.1.c]<br><br>"The [JLEA} on its own cannot promise or agree to any consideration by a Federal Prosecutor's Office or a Court in exchange for your cooperation, since the decision to confer any such benefit lies within the exclusive discretion of the Federal Prosecutor's Office and the Court. However, the [JLEA] will consider (but not necessarily act upon) a request by you to advise the appropriate Federal Prosecutor's Office or Court of the nature and extent of your assistance to the [JLEA]. [II.C.1.d]<br><br>"You have no immunity or protection from investigation, arrest or prosecution for anything you say or do, and the [JLEA] cannot promise or agree to such immunity or protection, unless and until you have been granted such immunity or protection in writing by a United States Attorney or his or her designee." [ II.C.1.e]<br><br>"You have not been authorized to engage in any criminal activity and could be prosecuted for any unauthorized criminal activity in which you have engaged or engage in the future" [II.C.1.f] | Agents no longer required to read immunity and authorized criminal activity instructions verbatim to all CIs but are required to review these instructions with CIs only where applicable. [II.C] |

| Confidential Informants | | |
|---|---|---|
| **Section** | **Previous Version 01/08/2001** | **Current Version 05/30/2002** |
| Instructions | Agents required to obtain signature from CIs acknowledging receipt and understanding of instructions unless inadvisable to do so for operational reasons. | Eliminates requirement that agents obtain CI's signature but still requires CI's verbal acknowledgement of receipt and understanding of instructions. CI's written acknowledgement is still required for otherwise illegal activity authorization and receipt of payment. [II.C.2] |

| Undercover Operations | | |
|---|---|---|
| **Section** | **Previous Version 11/13/1992** | **Current Version 05/30/2002** |
| **Part II. Definitions** | | |
| "Undercover Operation" – substantive contact | "A 'series of related undercover activities' generally consists of more than three separate contacts by an undercover employee with the individual(s) under investigation. However, undercover activity involving sensitive or fiscal circumstances constitutes an undercover operation regardless of the number of contacts involved." [II.B] | Replaces "contact" with "substantive contact" and defines latter term:<br><br>"[a] 'series of related undercover activities' generally consists of more than three separate substantive contacts by an undercover employee with the individual(s) under investigation. However, undercover activity involving sensitive or fiscal circumstances constitutes an undercover operation regardless of the number of contacts involved. A contact is 'substantive' if it is a communication with another person, whether by oral, written, wire, or electronic means, which includes information of investigative interest. Mere incidental contact, e.g., a conversation that establishes an agreed time and location for another meeting, is not a substantive contact within the meaning of these Guidelines." [II.B] |
| "Undercover Operation" – online communications | No Corresponding Text | Explains that multiple transmissions or e-mail messages can constitute a single contact. Factors considered in determining whether multiple online transmissions constitute single or multiple contacts include the time between transmissions, the number of transmissions, the number of interruptions, topical transitions, and the media by which the communications are exchanged. [II.B] |
| "Joint Undercover Operation" | No Corresponding Text | Defines term as an "[u]ndercover operation conducted jointly by the FBI and another law enforcement agency, except that an operation in which FBI participation is confined to contribution of limited financial or equipment resources or technical advice does not constitute a joint undercover operation." [II.F] |

| Undercover Operations | | |
|---|---|---|
| **Section** | **Previous Version 11/13/1992** | **Current Version 05/30/2002** |
| **Part III. General Authority and Purpose** | | |
| | "The FBI may use undercover activities and conduct undercover operations, pursuant to these Guidelines, that are appropriate to carry out its law enforcement responsibilities." [III] | Clarifies that undercover activities may be used in preliminary inquiries, general crimes investigations, and criminal intelligence investigations. [III] |
| | "[T]he FBI may participate in joint undercover activities with other law enforcement agencies and may operate a proprietary to the extent necessary to maintain an operation's cover or effectiveness. All joint undercover operations are to be conducted pursuant to these Guidelines. [III] | Specifies circumstances where FBI may rely upon another agency's authorization process. "If a joint undercover operation is under the direction and control of another federal law enforcement agency and is approved through a sensitive operations review process substantially comparable to the process under these Guidelines, the other agency's process may be relied on in lieu of the process under these Guidelines." [III] |
| **Part IV. Authorization of Undercover Operations** | | |
| General Approval Standards | Careful consideration must be given to risk of invasion of privacy or interference with privileged or confidential relationships. [IV.A] | Expands privacy considerations to include "any potential constitutional or other legal concerns." [IV.A] |

| Undercover Operations | | |
|---|---|---|
| **Section** | **Previous Version 11/13/1992** | **Current Version 05/30/2002** |
| UCOs Which May Be Approved by the SAC | No Corresponding Text | Adds note providing that the FBI should not hesitate to use lawful investigative techniques even if intrusive if circumstances warrant, especially with respect to terrorist offenses. "The gathering of evidence and information through undercover operations furthers the investigative objectives of detecting, preventing, and prosecuting crimes. (citations omitted). In furthering these objectives, the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (Part I) state that "[t]he 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." As with other investigative techniques, Special Agents in Charge should be guided by this principle in considering and approving undercover operations. The principle, as noted, applies with particular force where the undercover operation is directed to gathering information that will help to solve and prosecute terrorist offenses or prevent the future commission of acts of terrorism." [IV.B.1.b] |
| | Undercover expenditures may not exceed $40,000 ($100,000 in drug cases of which a maximum of $40,000 is for operational expenses). [IV.B.2] | Increases expenditure limits from $40,000 to $50,000 for Group II undercover expenditures ($100,000 in drug cases of which maximum of $ 50,000 is for operational expenses). [IV.B.2] |

| Undercover Operations | | |
|---|---|---|
| **Section** | **Previous Version 11/13/1992** | **Current Version 05/30/2002** |
| Operations Which Must Be Approved at FBIHQ | Fiscal circumstance (d): Require a reimbursement or compensation agreement with cooperating individuals or entities for services or losses incurred by them in aid of the operation (any reimbursement agreement entered into with third parties must be reviewed by the FBI's Legal Counsel Division) [IV.C.1.d] | Expands review of third party agreements to include Office of the Chief Contracting Officer. [IV.C.1.d] |
| | Sensitive circumstance (c): Section Chief of the FBIHQ White Collar Crimes Section must be consulted regarding conduct by certain non-sensitive officials. [IV.C.2.c] | Changes consultation designee to Section Chief of the FBIHQ Integrity in Government/Civil Rights Section, Criminal Investigative Division. [IV.C.2.c] |
| Criminal Undercover Operations Review Committee (Undercover Review Committee) - Sensitive Circumstances | "Activity that is proscribed by Federal, state, or local law as a felony or that is otherwise a serious crime -- but not including the purchase of stolen or contraband goods; the delivery or sale by the Government of stolen property whose ownership cannot be determined; the controlled delivery of drugs which will not enter commerce; the payments of bribes which are not included in the other sensitive circumstances; or the making of false representations to third parties in concealment of personal identity or the true ownership of a proprietary (this exemption does not include any statement under oath or the penalties of perjury)." [IV.C.2.g] | Clarifies that felony activity by an undercover employee qualifies as a "sensitive circumstance" requiring FBIHQ review and CUORC approval, and exempts such review for five or fewer money laundering transactions not to exceed maximum aggregate amount of $1 million. [IV.C.2.g] |
| | "Activities which could result in significant claims against the United States arising in tort, contract, or for compensation for the "taking" of property." [IV.C.2.n] | Adds potential for constitutional tort claims against government employees as a sensitive circumstance:<br>"Activities which create a realistic potential for significant claims against the United States arising in tort, contract, or for compensation for the "taking" of property, or a realistic potential for significant claims against individual government employees alleging constitutional torts." [IV.C.2.n] |
| | "The Director, Assistant Attorney General, or other official designated by them may refer any sensitive investigative matter, including informant, cooperating witness, and cooperating subject operations, to the Undercover Review Committee for advice, recommendation or comment, regardless of whether an undercover operation is involved." [IV.D.6] | Provides that SAC may submit an undercover operation for review by FBIHQ and the CUORC, regardless of whether sensitive circumstances are present. [IV.D.6] |

| Undercover Operations | | |
|---|---|---|
| **Section** | **Previous Version 11/13/1992** | **Current Version 05/30/2002** |
| Approval by the Director, Deputy Director, Designated Executive Assistant Director, or Designated Assistant Director | Excepting emergencies, only the Director, Deputy Director, or Associate Deputy Director-Investigations may approve undercover operations considered by CUORC for sensitive circumstances (l) or (m). [IV.E] | Authorizes a designated Executive Assistant Director to approve matters involving sensitive circumstances (l) and (m); reference to Associate Deputy Director of Investigations eliminated. [IV.E] |
| Application/ Notification to FBIHQ | *For TEIs, application must include "a statement why the infiltration or recruitment is necessary, a description of procedures to minimize any acquisition, retention, and dissemination of information that does not relate to the matter under investigation or to other authorized investigative activity." [IV.E.2.a.ii] | Requires "explanation of how any potential constitutional concerns and any other legal concerns have been addressed." [IV.E.2.a.ii] |
| | No Corresponding Text | Adds requirement that the FBI immediately notify the Deputy Attorney General whenever FBIHQ rejects an application and whenever the CUORC is unable to reach consensus concerning an application. [IV.E.4] |
| Duration of Authorization | "An undercover operation initially authorized by the SAC must be reauthorized by a designated Assistant Director, pursuant to paragraphs IV.C-F, if it lasts longer than 12 months or involves the expenditure of more than $40,000 ($100,000 in drug cases of which a maximum of $40,000 is for operational expenses), or such other amount that is set from time to time by the Director. No undercover operation approved at the field office level may continue for more than one year without obtaining approval at FBIHQ." [IV.G.4] | Increases expenditure limit from $40,000 to $50,000 for undercover expenditures and operational expenses. [IV.G.4] |
| Participation in Otherwise Illegal Activity By Undercover Employees | No Corresponding Text | Expands SAC authorization to include up to five money laundering transactions, not to exceed a maximum aggregate amount of $1 million. [IV.H.5.a.viii] |
| | Authorization by Director or Deputy Director required for otherwise illegal activity involving significant risk of violence or physical injury. [IV.H.5.c] | Includes designated Executive Assistant Director as authorizing official. [IV.H.5.c] |

| Undercover Operations | | |
|---|---|---|
| **Section** | **Previous Version 11/13/1992** | **Current Version 05/30/2002** |
| Interim/ Emergency Authorization | "In situations which require the prior written authorization of the SAC, the SAC may orally approve an undercover operation when he or she determines that a significant and unanticipated investigative opportunity would be lost were the time taken to prepare a written authorization." [IV.I.1] | Eliminates requirement that investigative opportunity be "unanticipated." [IV.I.1] |
| | "In situations which would otherwise require approval by the Director or Deputy Director, the SAC may approve an undercover operation when he or she determines that the initiation, extension, or renewal of an operation is imperative to protect life or prevent serious injury." [IV.I.2.b] | Authorizes SAC emergency approval for sensitive circumstances listed in IV.C.(2)(l) and (m) under certain conditions. "In situations which involve sensitive circumstance (l) or (m), the SAC may approve an undercover operation when he or she determines that the initiation, extension, or renewal of an operation is imperative to protect life or prevent serious injury." [IV.I.2.b] |
| | No Corresponding Text | Expands SAC emergency authorization to terrorism matters to avoid loss of investigative opportunity. "In situations which involve sensitive circumstance (l), or other investigative activity relating to terrorism, the SAC may approve an undercover operation when he or she determines that the initiation, extension, or renewal of an operation is necessary to avoid the loss of a significant investigative opportunity." [IV.I.2.c] |

| Undercover Operations | | |
|---|---|---|
| **Section** | **Previous Version 11/13/1992** | **Current Version 05/30/2002** |
| Interim/ Emergency Authorization | No Corresponding Text | Adds provision governing interim online undercover operations; in circumstances where continued online contact is essential to maintain credibility or avoid permanent loss of contact:<br>-SAC may authorize in writing interim operations for no longer than 30 days.<br>- FBIHQ must be notified if sensitive circumstances present.<br>-Full report of all online activity during period must be submitted to approving authority<br><br>During interim period, the undercover employee must:<br>-Maintain an accurate recording of all online communication;<br>-Avoid otherwise illegal activity;<br>-Maintain as limited an online profile as possible consistent with the need to accomplish stated objectives;<br>-Avoid physical contact with subjects;<br>-Take reasonable and necessary steps to protect third parties, commercial establishments, or government entities; and<br>-Cease if, during the 30-day period, a determination is made to disapprove the undercover operation. [IV.I.5] |
| **Part VI. Monitoring and Control of Undercover Operations** | | |
| Annual Report of the Undercover Review Committee | Records and summaries of undercover operations shall be made available for inspection by designee of the Associate or Deputy Attorney General and as appropriate of the Assistant Attorney General for the Criminal Division. [IV.E.1] | Deletes reference to Associate Attorney General. [IV.E.1] |
| | CUORC required to submit annual report to the Director, Attorney General, Associate or Deputy Attorney General, and the Assistant Attorney General for the Criminal Division. [VI.E.2] | Deletes reference to Associate Attorney General. [VI.E.2] |

# APPENDIX D

## USAO CRIMINAL DIVISION CHIEFS' VIEWS ON ADEQUACY OF FBI COORDINATION ON CONFIDENTIAL INFORMANT GUIDELINES ISSUES[1]

| Approval | Response | No. | Percent |
|---|---|---|---|
| 23. Are you aware of any situations in which the FBI has granted Tier I authorization to a CI without obtaining written approval from your Office? If yes, complete 23.a. and 23.b. | Yes | 0 | 0% |
| | No | 93 | 100% |

| Notification/Consultation | Response | No. | Percent |
|---|---|---|---|
| 29. The revised Guidelines on Confidential Informants require that in the event a CI is named in an electronic surveillance affidavit pursuant to Section III.D.1., the FBI must inform the prosecutor making the application and the court to which the application is made of the individual's actual status as a CI. (Section III.D.2.) Since 5/30/02, has a CI been named in an electronic surveillance affidavit in your Office? If yes, complete 29.a. | Yes | 25 | 27% |
| | No | 69 | 73% |
| 29a. If yes, how consistently has your Office received the appropriate notice from the FBI? | All appropriate cases | 23 | 88% |
| | Majority of cases | 2 | 8% |
| | Sometimes | 0 | 0% |
| | Rarely | 0 | 0% |

[1] This survey was an electronic questionnaire that was completed online through the Internet. Online respondents were required to answer each question presented; otherwise, they could not continue with the survey. However, several respondents did not complete the survey online, and instead submitted a written version via electronic mail or facsimile. Some of these respondents did not provide answers to some questions; as a result, the overall total number of respondents varies from question to question. There were a total of 96 respondents who provided answers to this survey.

Some questions required the respondent to answer follow-up questions that were automatically skipped without prompting the respondent if a certain response was entered. We instructed the respondents to rely exclusively on the navigation buttons provided within the survey program to go back and review and/or change previously entered answers and *not* to use the web browser's "back" and "forward" buttons. This was necessary because the survey's navigation buttons functioned within the confines of the survey by skipping questions when required, while use of the web browser's "back" and "forward" buttons simply re-displayed the pages previously accessed that remained in the browser's image cache. As a result, respondents who used their browser's navigation buttons could go back to change their answers to questions without affecting the responses to any relevant follow-up questions, thus producing inconsistent response totals within related questions.

| Notification/Consultation | Response | No. | Percent |
|---|---|---|---|
| | Never | 0 | 0% |
| | Don't know | 1 | 4% |
| 30. The revised Guidelines on Confidential Informants require that when the FBI has reasonable grounds to believe that a current or former CI is being prosecuted by, is the target of an investigation by, or is expected to become a target of an investigation by a federal prosecuting office for engaging in alleged felonious criminal activity, a SAC must immediately notify the chief federal prosecutor of that individual's status as a current or former CI. (Section IV.A.1.) Are you aware of situations in which the FBI has failed to notify the chief federal prosecutor in any of these circumstances? If yes, complete 30.a. through c. | Yes | 1 | 1% |
| | No | 93 | 99% |
| 31. Are you aware of circumstances in which a confidential informant who was then authorized to engage in either Tier 1 or Tier 2 otherwise illegal activity in the course of an undercover operation run by the FBI field office in your District engaged in *unauthorized illegal activity* since 5/30/02 (Section IV.B)? If yes, complete 31.a. through c. | Yes | 9 | 10% |
| | No | 85 | 90% |
| 31b. Do you believe that your Office and the FBI field office in your District have the same understanding of the circumstances requiring notification of the USAO of unauthorized illegal activity?[2] | Yes | 9 | 90% |
| | No | 1 | 10% |
| 32. Are you aware of circumstances in which a confidential informant who had no current authorization to engage in either Tier 1 or Tier 2 otherwise illegal activity engaged in *any criminal activity* in the course of an undercover operation run by the FBI field office in your District since 5/30/02 (Section IV.B)? If yes, complete 32.a. through c. | Yes | 1 | 1% |
| | No | 93 | 99% |

[2] The total number of responses corresponds to the number of respondents who answered "yes" to Question 31. Nine respondents answered "yes." One respondent apparently changed his or her answer from "yes" to "no" after responding to follow-up Question 31b, accounting for the incongruous number of expected responses to this question.

| Notification/Consultation | Response | No. | Percent |
|---|---|---|---|
| 32a. In the case of a confidential informant who had no current authorization to engage in either Tier 1 or Tier 2 otherwise illegal activity who engaged in any criminal activity in the course of an undercover operation run by the FBI field office in your District since 5/30/02, was the FBI's obligation to notify your Office immediately excused because a state or local prosecuting office in the District had filed charges against the confidential informant for the criminal activity and there was no basis for federal prosecution in your District?[3] | Yes | 2 | 67% |
| | No | 1 | 33% |
| 38. Please indicate the frequency of the following problems regarding the administration of Confidential Informants operated by the FBI field office in your District since 5/30/02: | Very frequently | 0 | 0% |
| | Occasionally | 1 | 1% |
| | Rarely | 16 | 17% |
| d) Inadequate or untimely notification to prosecutors of investigation or prosecution of Confidential Informants | Never | 63 | 67% |
| | Don't know | 14 | 15% |
| e) Inadequate or untimely notification to prosecutors of unauthorized illegal activity by Confidential Informants | Very frequently | 0 | 0% |
| | Occasionally | 1 | 1% |
| | Rarely | 17 | 18% |
| | Never | 61 | 65% |
| | Don't know | 15 | 16% |
| p) Failure to notify the appropriate federal prosecutor of unauthorized illegal activity by Confidential Informants | Very frequently | 0 | 0% |
| | Occasionally | 0 | 0% |
| | Rarely | 16 | 17% |
| | Never | 53 | 56% |
| | Don't know | 25 | 27% |
| 39. Please identify the impact of the following problems on the success of the Confidential Informant Program operated by the FBI field office in your District since 5/30/02: | Very serious | 0 | 0% |
| | Somewhat serious | 1 | 1% |
| | Occasional concern | 3 | 3% |
| f) Inadequate or untimely notification to prosecutors of investigation or prosecution | Minor concern | 13 | 14% |

[3] The total number of responses corresponds to the number of respondents who answered "yes" to Question 32. Only one respondent answered "yes." Two respondents apparently changed their answer from "yes" to "no" after responding to follow-up Question 32a, accounting for the incongruous number of expected responses to this question.

| Notification/Consultation | Response | No. | Percent |
|---|---|---|---|
| of Confidential Informants | No concern | 76 | 82% |
| g) Inadequate or untimely notification to prosecutors of unauthorized illegal activity by Confidential Informants | Very serious | 0 | 0% |
| | Somewhat serious | 0 | 0% |
| | Occasional concern | 5 | 5% |
| | Minor concern | 17 | 18% |
| | No concern | 71 | 76% |
| q) Failure to notify the appropriate federal prosecutor of unauthorized illegal activity by Confidential Informants | Very serious | 1 | 1% |
| | Somewhat serious | 0 | 0% |
| | Occasional concern | 7 | 8% |
| | Minor concern | 16 | 17% |
| | No concern | 68 | 74% |
| t) Failure to share information with federal prosecutor's office about Confidential Informant's activities in investigations in which the USAO is participating | Very serious | 1 | 1% |
| | Somewhat serious | 1 | 1% |
| | Occasional concern | 6 | 6% |
| | Minor concern | 17 | 18% |
| | No concern | 68 | 73% |

# APPENDIX E

# RECOMMENDATIONS

## CHAPTER THREE: THE ATTORNEY GENERAL'S GUIDELINES REGARDING THE USE OF CONFIDENTIAL INFORMANTS

### Develop and Implement a Compliance Plan

(1) Develop a compliance plan for its human source program and an implementation plan to put the plan into practice. The compliance plan should specify the strategies that the FBI will employ to ensure compliance with applicable Guidelines governing the recruitment, validation, and operation of human sources and address issues such as administrative support (e.g., field guides, standardized forms, and "user-friendly" Intranet resources), training, technology, guidance, and accountability.

### Provide Enhanced Administrative and Technical Support/Automation

(2) Develop standardized forms to capture the most significant requirements of the Confidential Informant Guidelines and the FBI's Manual of Investigative Operations and Guidelines (MIOG) for operating confidential informants, including a standardized "file review" cover sheet for Supervisory Special Agents to use in examining the files for adherence to the Confidential Informant Guidelines and MIOG provisions relating to confidential informants. The FBI should also create an electronic Confidential Informant User's Manual comparable to the Field Guide for Undercover and Sensitive Operations. That manual should include compliance checklists and the standardized forms recommended above. The FBI should consider other administrative improvements to support the Criminal Informant Program, including a standard electronic Criminal Informant Program tickler system that can be deployed in all field divisions to generate non-compliance notifications to field and Headquarters managers, and an updated Intranet web page that includes the current version of the Confidential Informant Guidelines and key Office of the General Counsel guidance memoranda concerning confidential informants.

(3) Institute procedures to determine whether state or local prosecuting offices have filed charges against confidential informants who engage in unauthorized illegal activity to determine whether notification must be provided to the U.S. Attorney's Office in accordance with § IV.B.1.a of the Confidential Informant Guidelines.

(4) Amend the forms used to authorize "otherwise illegal activity" to specify the thresholds referenced in § I.B.10 that distinguish Tier 1 from Tier 2 otherwise illegal activity.

**Make Personnel and Performance Plan Adjustments to Promote Adherence to the CI Guidelines**

(5) Revise the promotion policies and the performance plans for Special Agents and executive managers to indicate, where applicable, that compliance or overseeing compliance with the Confidential Informant Guidelines will be considered in employees' annual performance appraisals (in accordance with § I.I of the Confidential Informant Guidelines) and in promotion decisions.

(6) Evaluate the grade level of Special Agents who serve as Confidential Informant Coordinators and consider allowing Confidential Informant Coordinators to be elevated to a GS-14 supervisory level, particularly in larger field offices where the Coordinator is a full-time position. The FBI should also ensure that Confidential Informant Coordinators are supervised by personnel of a higher grade level who are familiar with the Criminal Informant Program and who have received training on the Confidential Informant Guidelines.

**Provide Necessary Training**

(7) Consider holding annual Informant Coordinator Conferences similar to those provided to Undercover Coordinators. The FBI should also consider opportunities for local, joint training with representatives from U.S. Attorneys' Offices, which could address topics such as Guidelines provisions requiring approval, concurrence, or notice to the U.S. Attorneys' Offices; the adverse consequences of Guidelines' violations from the standpoint of the prosecution and the FBI; and "lessons learned" from past cases.

(8) Review the training modules now used in New Agent Training, probationary training, and in-service training for Special Agents and Supervisory Special Agents to ensure that the Confidential Informant Guidelines' requirements and risks of operating confidential informants are explained.

(9) Include in the periodic training of Supervisory Special Agents a component or module on the importance of file reviews to the Criminal Informant Program. The training should also address frequently occurring violations of the Guidelines and MIOG provisions. A key objective of supervisory training should be on predictors of problems with confidential informants, such as long term confidential informants, confidential informants who have been assigned the same contact agents for an extensive period, confidential informants who are authorized to engage in otherwise illegal activity, confidential informants who have previously been deactivated "for cause," and confidential informants who have been arrested or engaged in other unauthorized illegal activity while working as confidential informants.

## CHAPTER FOUR: THE ATTORNEY GENERAL'S GUIDELINES ON FBI UNDERCOVER OPERATIONS

### Enhance the Role of Undercover Coordinators and Division Counsel

(10) Evaluate the grade level of Special Agents who serve as Undercover Coordinators and consider allowing Undercover Coordinators to be elevated to a GS-14 supervisory level, particularly in larger field offices where executive management deems it necessary to be a full-time position.

(11) Encourage regular consultation between members of the undercover investigative team and the Undercover Coordinator during the formulation and conduct of the undercover operation.

(12) Evaluate ways for the Undercover Coordinator to perform progress reviews at least every 90 days on undercover operations, a component of which should include an evaluation by senior managers, in consultation with Division Counsel and the Undercover Coordinator, of compliance with the Undercover Guidelines. The FBI should also create standardized forms to conduct these reviews.

(13) Establish policies that promote more consistent Division Counsel involvement in the development and implementation of undercover operations, and ensure that Division Counsel are advised of anticipated legal problems in undercover operations.

### Improve Guidance and Training

(14) Because neither the MIOG nor FBI field guides adequately address the issues below, provide guidance on the following:

- the meaning of "sensitive circumstances" relating to "systemic corruption" of governmental functions, and the "significant risk" of violence or physical injury to individuals pursuant to Undercover Guidelines §§ IV.C.2.b and IV.C.2.m, respectively;
- how to limit the scope of authorizations for otherwise illegal activity in undercover operations; and
- special concerns and compliance issues associated with task force participation.

(15) Identify ways to enhance Undercover Guidelines compliance training for field supervisors and undercover employees, including use of instructional CD-ROMs, web-based courses, and joint training with the U.S. Attorneys' Offices. Absent exigent circumstances, either as part of the certification of undercover employees or otherwise, the FBI should require undercover employees to complete undercover operation compliance training before participating in undercover operations. The FBI should also

ensure that all field supervisors who provide guidance pursuant to § VI.A of the Guidelines regarding preparation of undercover employees are familiar with undercover techniques, compliance requirements, and the Field Guide for Undercover and Sensitive Operations.

**Improve Internal Controls**

(16) As part of the Undercover Coordinator's certification currently provided for Group I and II undercover operation proposals, add a certification that the instructions set forth in § VI.A.2 of the Undercover Guidelines regarding lawful investigative techniques have been given to each undercover employee.

(17) Amend the Group I and Group II undercover operation proposals forms that currently provide information regarding the expected execution of the undercover operation to include a section: "Facts Pertinent to Violence Risk Assessment."

(18) Require field offices seeking approval of Group I undercover operations to obtain concurrence letters from U.S. Attorneys' Offices that meet the requirements of § IV.F.2.b of the Undercover Guidelines and amend § 4.8(5) of the Field Guide for Undercover and Sensitive Operations accordingly.

(19) Ensure that the Undercover and Sensitive Operations Unit has access to the Inspection Division's undercover operation audits.

## CHAPTER FIVE: ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS

**Preliminary Inquiries**

(20) Ensure compliance with the General Crimes Guidelines' requirements to obtain and document authorizations for the extension, conversion to full investigation, and closing of preliminary inquiries.

**Criminal Intelligence Investigations**

(21) Institute measures to ensure consistency in meeting and documenting the notification and reporting requirements provided in §§ III.A.5 and III.B.4 of the General Crimes Guidelines, including requiring FBI field offices to maintain in the relevant investigative file documentation of the notice of the opening of criminal intelligence investigations to DOJ's Counterterrorism, Organized Crime and Racketeering Sections, Office of Intelligence Policy and Review (OIPR), and the relevant U.S. Attorneys' Offices as required in racketeering enterprise investigations and terrorism

enterprise investigations. The FBI should also ensure that progress reports required by the Guidelines in terrorism enterprise investigations are provided to OIPR, DOJ's Counterterrorism Section, and FBI Headquarters.

(22) Discuss with DOJ how to reconcile § 100-2.3(3) of the MIOG, requiring Headquarters' concurrence with the initiation and renewal of terrorism enterprise investigations, with §§ III.B.4.a and b of the General Crimes Guidelines, which authorize field level initiation and renewal of these investigations.

**Part VI Counterterrorism Authorities**

(23) Require field level supervisory approval prior to the exercise of Part VI.A.2 authorities to visit public places or attend public events for the purpose of detecting or preventing terrorist activities, absent exigent circumstances.

(24) Develop a standardized form or a short e-mail template to be completed by case agents to document their use of the Part VI.A.2 authorities.

(25) In light of the survey responses of Division Counsel, consider whether (a) field office practices since May 30, 2002, regarding predication, collection, record retention, indexing, and dissemination of Part VI.A information, and the practices regarding utilization of "zero files" or other files to capture Part VI.A information, are in conformity with the Guidelines and FBI guidance; (b) there is a need for further guidance on predication, collection, record retention, indexing, dissemination, or other issues; and (c) FBI Headquarters managers should have access to data reflecting use of Part VI.A.2 authorities in order to be satisfied that these authorities are used in conformity with the Guidelines.

**CHAPTER SIX: PROCEDURES FOR LAWFUL, WARRANTLESS MONITORING OF VERBAL COMMUNICATIONS (CONSENSUAL MONITORING)**

(26) Ensure that required authorizations for consensual monitoring are obtained in advance and are appropriately documented.

(27) For monitorings that do not require DOJ approval, consult with DOJ to resolve whether the Consensual Monitoring Guidelines should be interpreted to authorize monitoring for more than 90 days (including up to "the duration of the investigation" as currently provided on Form FD-759), or whether the authorization is limited to 90 days. The resulting interpretation should be incorporated in the FBI's MIOG and communicated to the field.

## CHAPTER SEVEN: FBI AND DOJ COMPLIANCE OVERSIGHT AND ENFORCEMENT MECHANISMS

### Criminal Undercover Operations Review Committee (CUORC)

(28) Provide CUORC members, upon request, with access to copies of Inspection reports concerning undercover operations, the Undercover and Sensitive Operations Unit on-site reviews, and after-action reports of undercover operations.

(29) Consider ways for the Undercover and Sensitive Operations Unit to develop more complete information for the CUORC and other FBI components, such as conducting a periodic analysis of the patterns and trends found in its on-site reports, informing the CUORC members of any persistent Guidelines violations, and providing copies of its semi-annual report to all FBI Headquarters' operating Divisions, the Office of the General Counsel, and the Training Division.

### Confidential Informant Review Committee (CIRC)

(30) To assist CIRC members in evaluating the confidential informants within its purview and assist field and Headquarters managers in their supervisory responsibilities in overseeing the Criminal Informant Program, require that the Initial and Continuing Suitability Reports and Recommendations contain more thorough answers to the suitability questions, such as:

- a description of the confidential informants' legitimate source of income;
- the confidential informants' statistical accomplishments, including the number of indictments, convictions, Title III wiretap applications, and other indicia of informants' contributions;
- details on how confidential informants are in a position to obtain relevant information;
- details on the nature of any unauthorized illegal activity committed by confidential informants, including informants' criminal history records and the continuing suitability reports required to be completed in accordance with § II.A.2.b of the Confidential Informant Guidelines; and
- the informant records of any confidential informants who have been previously deactivated for cause by the FBI, including the reasons for deactivation and the field division operating the informants.

(31) Consider having the Human Intelligence Unit draft "lessons learned" from the CIRC's decisions, periodically communicate these lessons to field personnel, and incorporate them into training on the Confidential Informant Guidelines.

(32) Make available to CIRC members, upon request, copies of the Inspection Division's audits of the Criminal Informant Program (including any reinspection reports) and evaluations performed by the Human Intelligence Unit of compliance with the Confidential Informant Guidelines.

**Inspection Division**

(33) Revise Inspection Division checklists and interrogatories to increase inspection coverage of Guidelines-related issues.

(34) As part of the Inspection Division's triennial inspections of field and Headquarters' divisions, establish an audit examining the collection of information obtained from exercise of counterterrorism authorities pursuant to § VI.A.2 (Visiting Public Places and Events) of the General Crimes Guidelines.

(35) Provide more thorough and timely reporting of Attorney General Guidelines' violations by identifying in inspection reports the causes and gravity of compliance deficiencies; developing summary statistics to assist in determining when reinspections are appropriate; and automating key components of the inspection process.

(36) Increase inspections for the Criminal Informant Program and other programs that are priorities or experiencing significant problems by performing more frequent inspections at irregular intervals. The Inspection Division should also develop a standard for reinspections that accounts for the frequency and seriousness of the Attorney General Guidelines deficiencies identified during the regular inspection and develop a standard for determining when reinspections should be conducted that accounts for both the number and gravity of the deficiencies found. The Inspection Division and the Human Intelligence Unit should reinstate its Criminal Informant Program reinspection process.

(37) Address in employee performance appraisals the findings from Inspection Division inspections that identify either superior or deficient Attorney General Guidelines' compliance performance.

(38) Elevate egregious non-compliance with Attorney General Guidelines to an executive management finding in the inspection report rather than deferring that action until the next three-year inspection contingent on the detection of recurring, serious deficiencies.

**On-site Reviews by Program Offices**

(39) The Inspection Division and the Human Intelligence Unit should institute procedures that establish follow-up inspection measures to reinspections that indicate ongoing compliance problems, such as assigning a single Assistant Inspector in Place to conduct an additional inspection within the first six months following the reinspection.

(40) Modify the Undercover and Sensitive Operations Unit's on-site review data collection instrument to better address Guidelines compliance, including issues such as otherwise illegal activity, potential entrapment issues, and task force participation.

**FBI Disciplinary Process**

(41) Ensure that alleged Attorney General Guidelines' violations warranting potential discipline are referred to the FBI's Internal Investigations Section in a consistent fashion throughout the FBI.

(42) Ensure that the Inspection Division's standards for referring misconduct involving Attorney General Guidelines' violations are consistent with practices adopted by the Internal Investigations Section.

(43) Add separate offense codes for: (i) knowingly or recklessly failing to obtain proper authorization for a source's participation in otherwise illegal activity; (ii) knowingly or recklessly failing to obtain proper authorization to operate long term, high-level, privileged or media-affiliated confidential informants or other informants subject to special approval requirements; and (iii) knowingly or recklessly failing to operate long-term, high-level, privileged or media-affiliated confidential informants, or other informants subject to special approval requirements in accordance with the relevant Confidential Informant Guidelines and MIOG provisions.

**CHAPTER EIGHT: HOW THE FBI IMPLEMENTED THE MAY 30, 2002, REVISIONS TO THE ATTORNEY GENERAL'S INVESTIGATIVE GUIDELINES**

(44) Assign some person or unit at FBI Headquarters the responsibility to develop a plan to ensure proper and timely execution of Attorney General Guidelines' revisions and to coordinate implementation of the revisions over time.

(45) Distribute revised Attorney General Guidelines to Chief Division Counsel, together with a concise summary or listing of the changes, sufficiently in advance of the new Guidelines' effective date to allow field personnel to familiarize themselves with the revisions and to allow those Headquarters and field personnel who provide training on the revisions to develop training materials and a schedule for providing training. In

addition, near the effective date of the revision, the FBI should develop and distribute standardized forms and other administrative support tools, issue field guidance, and identify a Headquarters point of contact who can address questions concerning the revisions.

(46) Ensure that revisions to the MIOG accurately reflect any changes to the Attorney General Guidelines and are made on or about the effective date of such changes.

(47) Make appropriate changes to the MIOG to reconcile the discrepancies between the Attorney General Guidelines and the MIOG that are identified in this report.

# APPENDIX F

## DISCREPANCIES BETWEEN THE ATTORNEY GENERAL'S INVESTIGATIVE GUIDELINES AND FBI POLICY MANUALS

| Registration of Confidential Informants | |
|---|---|
| **Attorney General's Guidelines Regarding the Use of Confidential Informants** | **Manual of Investigative Operations & Guidelines (Part 1)** |
| II.B. After a Field Manager has approved an individual as suitable to be a CI, the individual shall be registered with that JLEA as a CI. In registering a CI, **the JLEA shall, at a minimum, document or include the following in the CI's files:**<br>1. a photograph of the CI;<br>2. the JLEA's efforts to establish the CI's true identity;<br>3. the results of a criminal history check for the CI;<br>4. the Initial Suitability Report and Recommendation;<br>5. any promises or benefits, and the terms of such promises or benefits, that are given a CI by a JLEA or any other law enforcement agency (if available to the JLEA);<br>6. **any promises or benefits, and the terms of such promises or benefits, that are given a CI by any FPO or any state or local prosecuting office (if available to the JLEA);** and<br>7. all information that is required to be documented in the CI's files pursuant to these Guidelines (e.g., the provision of the instructions set forth in the next paragraph). (emphasis added) | 137-5(3)(d).[1] In addition to those records generated during the SI, the following additional information, must be located in the file:<br>1. A photograph of the person;<br>2. Results of a criminal history check for the CI;<br>3. Any promises or benefits, and the terms of such promises or benefits, that are given a CI by the FBI or any other law enforcement agency (if available); (Also see AGG, § I (C))<br>4. All information that is required to be documented in the CI's files pursuant to §§ 137-6 (1) through (3). (AGG, § II (C)(1)-(2)).<br><br>Effective date: 01/14/2002 |
| **Contingency Payments to Confidential Informants** | |
| **Attorney General's Guidelines Regarding the Use of Confidential Informants** | **Manual of Investigative Operations & Guidelines (Part 1)** |
| III.B.2. Under no circumstances shall any payments to a CI be contingent upon the conviction or punishment of any individual. | No corresponding provision for contingency payments. |

[1] The MIOG requires the initial Suitability Report and Recommendation to list the CI's name, alias(s), and date and place of birth. MIOG § 137-5(1). We construe the CI Guidelines to require a description of the efforts the JLEA took to obtain this information.

| Deactivation of Confidential Informants | |
|---|---|
| **Attorney General's Guidelines Regarding the Use of Confidential Informants** | **Manual of Investigative Operations & Guidelines (Part 1)** |
| V.A. A JLEA that determines that a CI should be **deactivated for cause or for any other reason** shall immediately:<br>1. deactivate the individual;<br>2. document the reasons for the decision to deactivate the individual as a CI in the CI's files;<br>3. if the CI can be located, notify the CI that he or she has been deactivated as a CI and obtain documentation that such notification was provided in the same manner as set forth in paragraph (II)(C)(2); and<br>4. if the CI was authorized to engage in Tier 1 or Tier 2 Otherwise Illegal Activity pursuant to paragraph (III)(C)(2)(a)-(b), revoke that authorization under the provisions of paragraph (III)(C)(7). (emphasis added) | 137-15(12)(a). When a CI is being closed, an EC will be generated which will include the following:<br>. . . .<br>137-15(12)(4). **Whether the CI has been notified that they have been deactivated** and any authorization to participate in otherwise illegal activity has been revoked. If authorized for otherwise illegal activity, written acknowledgement by the CI of deactivation or two witnesses to the fact that the CI orally acknowledged his/her deactivation.<br>137-15(14). If a CI is **closed for cause**, the following must be done immediately:<br>a) Appropriate notification shall be made to the CI, in person, if he/she can be reasonably located;<br>b) Document the reasons for the decision to deactivate the individual as a CI in the CI's file;<br>c) If the CI was authorized to engage in Tier 1 or Tier 2 Otherwise Illegal Activity, the CI will be advised that the authority to participate in Otherwise Illegal Activity has been revoked. (AGG, § V (A))<br>d) Such notification of closure for cause shall be made by two Agents or an Agent and another "approved" law enforcement officer. Approved law enforcement officer means a task force officer or law enforcement officer to whom disclosure authority has previously been authorized. The notification and all attempts to notify the CI will be documented in writing. (emphasis added).<br>Effective date: 01/14/2002 |

| Preparation of Undercover Employees, Informants, and Cooperating Witnesses | |
|---|---|
| **Attorney General's Guidelines Regarding FBI Undercover Operations** | **Field Guide to Undercover and Sensitive Operations (July 25, 2003)** |
| VI.A.1. Prior to the investigation, the SAC or a designated Supervisory Special Agent shall review with each undercover employee the conduct that the undercover employee is expected to undertake and conduct that may be necessary during the investigation. **The SAC or Agent shall discuss with each undercover employee any of the sensitive or fiscal circumstances specified in § IV.C(1) or (2) that are reasonably likely to occur.** (emphasis added) | 10.2(1). The AGG, Section VI.A, requires the SAC or a designated supervisor, to discuss with all of the UCEs, informants, or cooperating witnesses involved in a UCO what is acceptable conduct during the UCO. Specifically, each UCE is to be instructed that he/she shall not participate in any act of violence except in self-defense; initiate or institute any plan to commit criminal acts; use unlawful investigative techniques to obtain information or evidence; or engage in any conduct that would violate any FBI, AGG or DOJ policy or restriction on investigative techniques or conduct by an FBI employee. The UCE will also be informed that except in an emergency situation, he/she shall not participate in any illegal activity for which authorization has not yet been obtained. The UCE will be informed that if a UCE learns persons under investigation intend to commit a violent crime, he/she shall try to discourage the violence. The UCE(s) shall also be instructed on the legal issues concerning entrapment. |

<table>
<tr><th colspan="2">Application/Notification to FBIHQ, Sensitive Circumstances</th></tr>
<tr><th>Attorney General's Guidelines Regarding FBI Undercover Operations</th><th>Field Guide to Undercover and Sensitive Operations (July 25, 2003)</th></tr>
<tr><td>IV.F.2.b. Applications for approval of undercover operations involving sensitive circumstances listed in paragraph C(2) shall also include the following information:<br>(b) A letter from the appropriate Federal prosecutor indicating that he or she has reviewed the proposed operation, including the sensitive circumstances reasonably expected to occur, agrees with the proposal and its legality, and will prosecute any meritorious case that has developed. The letter should include a finding that the proposed investigation would be an appropriate use of the undercover technique and that the potential benefits in detecting, preventing, or prosecuting criminal activity outweigh any direct costs or risks of other harm.</td><td>4.2(3)(B). A letter from the appropriate federal prosecutor indicating that he or she has reviewed the proposed operation, including the sensitive circumstances reasonably expected to occur, agrees with the proposal and its legality, and will prosecute any meritorious case that has developed. The letter should also include a statement concerning the propriety of the UCO and the legal sufficiency and quality of evidence that is being produced by the activity. The letter should be dated within 30 days of the scheduled Criminal Undercover Operations Review Committee (CUORC) meeting.</td></tr>
<tr><th colspan="2">Authorizations for Openings and Renewals of Terrorism Enterprise Investigations</th></tr>
<tr><th>Attorney General's Guidelines Regarding General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations</th><th>Manual of Investigative Operations & Guidelines (Part 1)</th></tr>
<tr><td>III.B.4.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 . . . .<br>III.B.4.b. Renewal authorization [for terrorism enterprise investigations] shall be obtained from the SAC with notification to FBIHQ.</td><td>100-2.3(3) With regard to full-field terrorism enterprise investigations of domestic terrorism, it is hereby the policy of the CTD that, consistent with the revised AGG, a full-field terrorism enterprise investigation may be authorized by an SAC only with concurrence of the appropriate CTD Section Chief at FBIHQ who has program responsibility for the type of case opened (domestic or international). . . .<br>Effective Date: 07/09/2003</td></tr>
</table>

| Use of Mail Covers in Preliminary Inquiries | |
|---|---|
| **Attorney General's Guidelines Regarding General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations** | **Manual of Investigative Operations & Guidelines (Part 2)** |
| II.B.5. All lawful investigative techniques may be used in an inquiry except:<br>(a) Mail openings; and<br>(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). | 10-6.2(7). Requests for mail covers should not be submitted in preliminary criminal inquiry investigations. ("The Attorney General's Guidelines on General Crimes, Racketeering Enterprises [sic], and Terrorism Enterprise Investigations," effective May 30, 2002.)<br>Effective Date: 04/04/2003 |

| Duration of Consensual Monitoring | |
|---|---|
| **Attorney General's Guidelines Regarding Procedures for Lawful, Warrantless Monitoring of Verbal Communications** | **Manual of Investigative Operations & Guidelines (Part 2)** |
| III.A Required Information The following information must be set forth in any request to monitor an oral communication pursuant to part II.A [Investigations Where Written Department of Justice Approval is Required]:<br>. . .<br>(6) Time. **The request must state the length of time needed for the monitoring. Initially, an authorization may be granted for up to 90 days from the day the monitoring is scheduled to begin.** If there is the need for continued monitoring, extensions for additional periods of up to 90 days may be granted.<br><br>V. Procedures for Consensual Monitoring Where No Written Approval Is Required<br>. . .<br>Records are to be maintained by the involved departments or agencies for each consensual monitoring that they have conducted. **These records are to include the information set forth in part III.A. above.** | 10-10.3(1). Nontelephonic Consensual Monitoring (NTCM) in criminal matters may be approved by the SAC/ASAC**, for the duration of the investigation**, except when one or more of the six sensitive circumstances is present. Requests for authority to conduct consensual monitoring when any of the six sensitive circumstances are present will be submitted in writing to FBIHQ for Department of Justice approval in ROUTINE situations. (emphasis added)<br><br>10-10.3(3). SAC/ASACs may authorize NTCM usage **for the duration of nonsensitive investigations** so long as the circumstances under which the authority was granted (i.e., the subject matter, the consenting party or parties to the interception, and the judicial district wherein monitoring will take place) do not substantially change—the authorization will remain valid. Where such changes are noted, consideration should be given by the SAC/ASACs to determine whether or not the NTCM authority should continue or whether new authority |

| | |
|---|---|
| | obtained.<br>Effective date: 09/30/2002 |

| **Emergency Procedures for Consensual Monitorings That Do Not Require DOJ Approval** | |
|---|---|
| **Attorney General's Guidelines Regarding Procedures for Lawful, Warrantless Monitoring of Verbal Communications** | **Manual of Investigative Operations & Guidelines (Part 2)** |
| V. [E]ach department or agency shall establish procedures for emergency authorizations in cases involving non-sensitive circumstances similar to those that apply with regard to cases that involve the sensitive circumstances described in part III.D, including obtaining follow-up oral advice of an appropriate attorney as set forth above concerning the legality and propriety of the consensual monitoring. | No implementing provisions. |

# APPENDIX G

# FBI RESPONSE TO OIG RECOMMENDATIONS

**Recommendations:**

**(1) Develop a compliance plan for its human source program and an implementation plan to put the plan into practice. The compliance plan should specify the strategies that the FBI will employ to ensure compliance with applicable Guidelines governing the recruitment, validation, and operation of human sources and address issues such as administrative support (e.g., field guides, standardized forms, and "user-friendly" Intranet resources), training, technology, guidance, and accountability.**

**FBI Response:** The FBI concurs with this recommendation and has begun implementing the changes. The Directorate of Intelligence (DI) is re-engineering the entire Confidential Human Source Program with emphasis on improving compliance with AG Guidelines and FBI policy.

As the Intelligence Program Manager within the FBI, the DI is developing new guidelines, policies, and processes for the utilization of confidential human sources that reduce burdensome paperwork and standardize source administration procedures. The DI drafted two new manuals for which approval is pending. First, a Confidential Human Source Manual, that contains one set of guidelines for all confidential human sources, consolidates language currently used in seven different source manuals and standardizes requirements for source administration. Second, a Confidential Human Source Validation Manual, that includes a standard, FBI-wide Confidential Human Source Validation Review Process and provides guidance for agents and supervisory personnel to develop and continually evaluate sources throughout the lifetime of the source's operation.

The proposed technology for automating the entire Confidential Human Source workflow process will standardize administrative processes, provide guidance to first-line supervisors who oversee all aspects of source administration and operation, and increase the ability of the FBI to track resources, historical data, and trends developing in the human source program. We expect this automation to reduce if not completely eliminate compliance errors with AG Guidelines and internal Bureau policies.

A new training initiative will include several additional hours of Confidential Human Source training for new agents, in addition to comprehensive advanced training for agents, supervisors and Human Source Coordinators in the field offices. For over six months, DI has coordinated closely with other FBI Headquarters entities, and the DOJ in order to finalize guidelines, technology and administrative support procedures. Phase one of the Confidential Human Source Re-engineering Project is expected to be completed in January 2006 and will include initial manual changes and information technology testing. Phase two will commence in April 2006 and will enable the FBI, through automation, to standardize the workflow process. In addition, AG Guidelines requirements will be built into the automated workflow with the goal of reducing significantly, if not entirely, compliance errors with AG Guidelines and FBI policies.

**(2) Develop standardized forms to capture the most significant requirements of the Attorney General Guidelines and the FBI's Manual of Investigative Operations and Guidelines (MIOG) for operating confidential informants, including a standardized "file review" cover sheet for supervisory special agents to use in examining the files for adherence to the Confidential Informant Guidelines and MIOG provisions relating to confidential informants. The FBI should also create an electronic Confidential Informant User's Manual comparable to the Field Guide on Undercover and Sensitive Operations. That manual should include compliance checklists and the standardized forms recommended above. The FBI should consider other administrative improvements to support the Criminal Informant Program, including a standard electronic Criminal Informant Program tickler system that can be deployed in all field divisions to generate non-compliance notifications to field and Headquarters managers, and an updated Intranet web page that includes the current version of the Confidential Informant Guidelines and key Office of General Counsel guidance memoranda concerning Confidential Informants.**

**FBI Response:** The FBI concurs with this recommendation. We agree that standardized forms and file review cover sheets will decrease the instances of non-compliance with the AG Guidelines and FBI policy. This is a major component of our Confidential Human Source Re-engineering initiative. Our automation initiative provides agents and supervisors with electronic templates that relate to all aspects of human

source administration and validation. The proposed templates promote adherence to AG Guidelines and FBI policies through built-in features that prevent users from proceeding without completing critical areas of the template, and through icons and links that allow agents to simultaneously access relevant portions of the human source manuals for reference purposes.

In April 2005, DI updated its Human Intelligence Planning and Policy Unit Intranet web page for human source information. The site includes human source guidelines and policies, administrative samples, project updates, personnel assignments and press releases. Based on previously described proposals to improve administrative support, we anticipate that the "Confidential Informant User's Manual" recommendation will be satisfied. In the interim, we will consider creating and implementing stop-gap uniform standardized forms throughout the FBI.

**(3) Institute procedures to determine whether state or local prosecuting offices have filed charges against Confidential Informants who engage in unauthorized illegal activity to determine whether notification must be provided to the U.S. Attorney's Office in accordance with Section IV.B.l.a of the Confidential Informant Guidelines.**

**FBI Response**: The FBI concurs that such procedures are desirable and will explore how best to accomplish this goal recognizing that a field office's ability to be informed of such matters may vary widely from jurisdiction to jurisdiction and recognizing, as well, that any such policy must be consistent with operational security and the protection of source identity.

The current AG Guidelines and FBI policy require a Special Agent in Charge (or the equivalent) to immediately notify an appropriate Chief Federal Prosecutor (CFP) of a CI's unauthorized illegal activity. Notification must be made to: (1) the CFP whose District is located where the criminal activity primarily occurred, unless a state or local prosecuting office in that District has filed charges against the CI for the criminal activity and there clearly is no basis for federal prosecution (Section IV.B.1.a); (2) the CFP, if any, whose District is participating in the conduct of an investigation that is utilizing the "active" CI; and (3) the CFP, if any, who authorized the CI to engage in Tier 1 otherwise illegal activity.

Determining whether a state or local prosecutor filed charges against a CI is the responsibility of the case agent handling the CI. Case agents conduct periodic criminal history record checks, maintain contact with CIs, and conduct ongoing background investigations of CIs in order to determine whether a CI engages in UIA. The first-line supervisor of the agent is responsible for ensuring the CFP is properly notified after UIA by a CI occurs, if required.

To better assist agents and supervisors with tracking notifications to the U.S. Attorney's Office, DI will consider designing a standard 90-day file review format that prompts the first-line supervisor to ensure the following documentation is contained in the file, if applicable: (1) the nature of any UIA by a source during the 90-day period under review; (2) the status and/or disposition of any charges filed by state or local prosecutors related to the UIA; and (3) the name of the CFP notified and date of notification. The new file review format will also reflect whether the CI's assistance is utilized in a current federal prosecution and whether the CI has authorization to engage in OIA. Appropriate manual revisions and re-engineering efforts will be undertaken in order to implement this new requirement.

**(4) Amend the forms used to authorize "otherwise illegal activity" to specify the thresholds referenced in Sections I.B. 10 that distinguish Tier 1 from Tier 2 otherwise illegal activity.**

**FBI Response:** The FBI concurs with this recommendation. Implementing Bureau-wide standardized forms that include the definitions of Tier 1 OIA and Tier 2 OIA, and prompt agents to provide specific information about the anticipated criminal activity, will provide useful guidance for agents and supervisors.

The threshold information from the U.S. Sentencing Guidelines may be too voluminous to include on a paper form. Alternatively, the threshold information can be accessible to FBI employees through the HIU's Intranet web page and built-in links to the proposed automated re-engineering system. Appropriate manual revisions and re-engineering efforts will be undertaken to implement this new requirement.

**(5) Revise the promotion policies and the performance plans for Special Agents and executive managers to indicate, where applicable, that compliance or overseeing compliance with the**

**Confidential Informant Guidelines will be considered in employees' annual performance appraisals (in accordance with Section I.I of the Confidential Informant Guidelines) and in promotion decisions.**

**FBI Response:** The FBI concurs with this recommendation. The current promotion policy and performance plan mandate that all FBI GS-10 to GS-15 employees comply with the AG Guidelines. Although the policy does not single out one specific set of AG Guidelines, e.g. "Confidential Informant Guidelines," the FBI believes this mandated element is addressed sufficiently because it encompasses all applicable AG Guidelines. The Bureau will take steps to enforce the policy and hold accountable agents who fail inordinately in matters of compliance.

**(6) Evaluate the grade level of Special Agents who serve as Confidential Informant Coordinators and consider allowing Confidential Informant Coordinators to be elevated to a GS-14 supervisory level, particularly in larger field offices where the Coordinator is a full-time position. The FBI should also ensure that that Confidential Informant Coordinators are supervised by personnel of a higher grade level who are familiar with the Criminal Informant Program and who have received training on the Confidential Informant Guidelines.**

**FBI Response:** The FBI concurs with this recommendation and will conduct the review.

**(7) Consider holding annual Informant Coordinator Conferences similar to those provided to Undercover Coordinators. The FBI should also consider opportunities for local, joint training with representatives from U.S. Attorneys' Offices, which could address topics such as Guidelines provisions requiring approval, concurrence, or notice to the U.S. Attorneys' Offices; the harm of Guidelines' violations from the standpoint of the prosecution and the FBI; and "lessons learned" from past cases.**

**FBI Response**: The FBI concurs with this recommendation. However, we ask that the text of the OIG report include the following in-service training provided by the Asset/Informant Unit:

TITLE OF COURSE: INFORMANT DEVELOPMENT AND MANAGEMENT, CIVIL RIGHTS UNIT IN-SERVICE, FBI ACADEMY
DATE: 01/08/2003

NUMBER OF ATTENDEES: 45
ATTENDEES: Supervisory Special Agents, Special Agents & Task Force Officers

TITLE OF COURSE: EXTRATERRITORIAL DESIGNATION AND SENSITIVE CIRCUMSTANCES, S-VISA PROGRAM REVIEW, SPBP PROGRAM REVIEW, CRITICAL SKILLS DEVELOPMENT, FBI HQ
DATE: 02/13/2003
NUMBER OF ATTENDEES: 100
ATTENDEES: Supervisory Special Agents

TITLE OF COURSE: INFORMANT DEVELOPMENT AND MANAGEMENT, ATLANTA DIVISION
DATE: 05/15/2003
NUMBER OF ATTENDEES: 50
ATTENDEES: Supervisory Special Agents, Special Agents & Task Force Officers

TITLE OF COURSE: INFORMANT DEVELOPMENT AND MANAGEMENT IN-SERVICE, FBI ACADEMY
DATES: 06/23 -27/03
NUMBER OF ATTENDEES: 56
ATTENDEES: Supervisory Special Agents and Special Agents

TITLE OF COURSE: ASSET/INFORMANT DEVELOPMENT AND POLICY, USOU IN-SERVICE, FBI ACADEMY
DATE: 06/25/2003
NUMBER OF ATTENDEES: 48
ATTENDEES: Special Agents and Task Force Officers

TITLE OF COURSE: INFORMANT DEVELOPMENT AND MANAGEMENT, LAS VEGAS DIVISION
DATES: 08/12 - 13/2003
NUMBER OF ATTENDEES: 70
ATTENDEES: Supervisory Special Agents, Special Agents & Task Force Officers

TITLE OF COURSE: INFORMANT DEVELOPMENT, COLUMBIA DIVISION
DATES: 8/13/2003
NUMBER OF ATTENDEES: 50
ATTENDEES: Supervisory Special Agents, Special Agents & Task Force Officers

TITLE OF COURSE: INFORMANT DEVELOPMENT, DENVER DIVISION
DATES: 9/8-12/2003
NUMBER OF ATTENDEES: 50

ATTENDEES: Supervisory Special Agents, Special Agents & Task Force Officers

TITLE OF COURSE: USOU IN-SERVICE, FBI ACADEMY, CIP POLICY
DATES: 9/17/2003
NUMBER OF ATTENDEES: 50
ATTENDEES: Special Agents and Task Force Officers

TITLE OF COURSE: DHS PAROLE CONFERENCE, SPBP MATTERS- NEW ORLEANS
DATES: 9/23-24/2003
NUMBER OF ATTENDEES: APPROX 150
ATTENDEES: Special Agents & Other Law Enforcement Officials

TITLE OF COURSE: CIP (ANCHORAGE DIVISION)
DATES: 9/30/2003
NUMBER OF ATTENDEES: 50
ATTENDEES: Supervisory Special Agents, Special Agents & Task Force Officers

TITLE OF COURSE: INFORMANT DEVELOPMENT, LITTLE ROCK DIVISION
DATES: 10/09/2003
NUMBER OF ATTENDEES: 50
ATTENDEES: Supervisory Special Agents, Special Agents & Task Force Officers

TITLE OF COURSE: INFORMANT DEVELOPMENT, LOUISVILLE DIVISION
DATES: 10/24-26/2003
NUMBER OF ATTENDEES: 50
ATTENDEES: Supervisory Special Agents, Special Agents & Task Force Officers

TITLE OF COURSE: INFORMANT DEVELOPMENT, ANCHORAGE DIVISION
DATES: 10/29 - 30 /2003
NUMBER OF ATTENDEES: 45
ATTENDEES: Supervisory Special Agents, Special Agents & Task Force Officers

TITLE OF COURSE: INFORMANT DEVELOPMENT SEMINAR (A/IU), FBI ACADEMY
DATES: 10/26-31/2003
NUMBER OF ATTENDEES: 50
ATTENDEES: Special Agents

TITLE OF COURSE: CIVIL RIGHTS IN-SERVICE (HQ), FBI ACADEMY
DATES: 11/06/2003
NUMBER OF ATTENDEES: 45
ATTENDEES: Special Agents

TITLE OF COURSE: BACK TO BASICS, FBIHQ
DATES: 11/21/2003 (TWO SESSIONS)
NUMBER OF ATTENDEES: APPROX 100
ATTENDEES: Executive Assistant Directors, Assistant Directors, Deputy Assistant Directors & Supervisory Special Agents

TITLE OF COURSE: BACK TO BASICS, FBIHQ
DATES: 12/05/2003 (TWO SESSIONS)
NUMBER OF ATTENDEES: APPROX 100
ATTENDEES: Executive Assistant Directors, Assistant Directors, Deputy Assistant Directors & Supervisory Special Agents

TITLE OF COURSE: BACK TO BASICS, FBIHQ
DATES: 12/08/2003
NUMBER OF ATTENDEES: APPROX 100
ATTENDEES: Executive Assistant Directors, Assistant Directors, Deputy Assistant Directors & Supervisory Special Agents

TITLE OF COURSE: BACK TO BASICS, FBIHQ
DATES: 12/17/2003
NUMBER OF ATTENDEES: APPROX 100
ATTENDEES: Executive Assistant Directors, Assistant Directors, Deputy Assistant Directors & Supervisory Special Agents

TITLE OF COURSE: BACK TO BASICS, FBIHQ
DATES: 01/08/2004
NUMBER OF ATTENDEES: APPROX 100
ATTENDEES: Executive Assistant Directors, Assistant Directors, Deputy Assistant Directors & Supervisory Special Agents

TITLE OF COURSE: HUMAN INTELLIGENCE DEVELOPMENT AND OPERATIONS IN-SERVICE - ADVANCED, FBI ACADEMY
DATES: 02/22 - 26/2004
NUMBER OF ATTENDEES: 13
ATTENDEES: Special Agents

TITLE OF COURSE: CIP POLICY, DRUG IN-SERVICE
DATES: 06/24/2004
NUMBER OF ATTENDEES: 40
ATTENDEES: Special Agents

TITLE OF COURSE: CIP POLICY – BEST PRACTICES
DATES: 07/15/2004
NUMBER OF ATTENDEES: 18
ATTENDEES: Assistant Directors, Deputy Assistant Directors and Assistant Special Agents in Charge

Note: This list excludes training provided to foreign law enforcement authorities, training that focused primarily on national security assets, and CIP training conducted after July 31, 2004. The former Asset/Informant Unit (A/IU), currently called the HIU, also hosted a Coordinator's Conference in August 2004.

**(8) Review the training modules now used in New Agent Training, probationary training, and in-service training for Special Agents and Supervisory Special Agents to ensure that the key Confidential Informant Guidelines requirements and risks of operating confidential informants are explained.**

**FBI Response**: The FBI concurs with this recommendation. The HIU and the Training Division are updating training modules in conjunction with the Confidential Human Source Re-engineering Initiative. In the interim, DI will review all human source training modules at the FBI Academy to ensure current requirements and risks of operating CIs are explained fully. Additionally, in the future, Confidential Human Source Training Presentations will be available to field offices via the Intranet web page.

**(9) Include in the periodic training of Supervisory Special Agents a component or module on the importance of file reviews to the Criminal Informant Program. The training should also address frequently occurring violations of the Guidelines and MIOG provisions. A key objective of supervisory training should be on predictors of problems with confidential informants, such as long term confidential informants, confidential informants who have been assigned the same contact agents for an extensive period, confidential informants who are authorized to engage in otherwise illegal activity, confidential informants who have previously been deactivated "for cause," and confidential informants who have been arrested or engaged in other unauthorized illegal activity while working as confidential informants.**

**FBI Response:** The FBI concurs with this recommendation and has begun implementation. In April 2005, the DI provided specific guidance for conducting Confidential Human Source file reviews to FBI Headquarters Supervisory Special Agents who are en route to field supervisory positions. Emphasis was placed on recurring violations of the AG Guidelines and MIOG provisions. Regular training and training materials will be made available to field office supervisory personnel in the future.

A new training initiative is underway which will include several additional hours of human source training for new agents, in addition to comprehensive advanced training for agents, supervisors and Human Source Coordinators in the field offices. DI anticipates that a new training curriculum will be developed by early 2006.

**(10) Evaluate the grade level of Special Agents who serve as Undercover Coordinators and consider allowing Undercover Coordinators to be elevated to a GS-14 supervisory level, particularly in larger field offices where executive management deems it necessary to be a full-time position.**

**FBI Response**: The FBI concurs with this recommendation and will conduct the evaluation.

**(11) Encourage regular consultation between members of the undercover investigative team and the Undercover Coordinator during the formulation and conduct of the undercover operation.**

**FBI Response**: The FBI concurs with this recommendation. Proper and effective coordination between the undercover team and all facets of the FBI's undercover program are essential to an effective, efficient, safe and successful investigation. Communication among key players in the undercover operation should occur throughout the undercover process.

The FBI's Field Guide on Undercover Operations (FGUSO) recognizes the importance of regular consultation among members of the undercover team. Recently, the Undercover and Sensitive Operations Unit (USOU) determined that communication is enhanced with the addition of an intelligence analyst and a field office Reports Officer to the undercover team. The undercover investigative team presently includes the squad supervisor, case agent, contact agent, undercover employee, account or financial analyst. The team is augmented by the Chief Division Counsel (CDC), Asset Forfeiture Coordinator, Financial Manager, Undercover Coordinator and the Special Agent in Charge (SAC).

Section 10 of the FBI's FGUSO specifically describes the responsibilities and conduct of undercover operation personnel. For example, it notes that the SAC agrees that he or she ". . . will meet regularly with the undercover agents . . . ," and ". . . the . . . will maintain contact with the undercover team. . . ." FGUSO outlines the roles and responsibilities of

the various other components of the undercover investigative team.

In addition to the existing policy, USOU provides training and conducts on-site reviews of undercover operations to ensure regular consultation occurs within the field office. Training now exists for all members of the undercover investigative team. Such training is in undercover certification courses, Group I writing seminars and FBI executive briefings at the field level during on-sites and at the FBIHQ level during new SAC orientations.

The FBI will add language to Section 10 of the FGUSO which outlines responsibilities of the Undercover Coordinator. It will include language emphasizing the need for ongoing consultation between the Undercover Coordinator and the undercover teams. The FBI will continue to send this message through training, undercover reviews and executive level briefings.

**(12) Evaluate ways for the Undercover Coordinator to perform progress reviews at least every 90 days on undercover operations, a component of which should include an evaluation by senior managers, in consultation with Division Counsel and the Undercover Coordinator, of compliance with the Undercover Guidelines. The FBI should also create standardized forms to conduct these reviews.**

**FBI Response**: The FBI concurs with this recommendation, as qualified below. Currently, the FBI employs a management tool known as a file review in all of its investigations. In the file review process, a field supervisor who maintains authority over a particular case agent reviews that agent's case file at least once every 90 days, sometimes sooner. The supervisor uses a standard FBI form to conduct this review and ensure compliance with all laws, policies and procedures, including those related to undercover matters.

Once the FBI supervisor completes his or her review of the agent's investigations (including those employing the undercover technique), the results of the file review are maintained for a period of time. They are also reviewed by an Assistant Special Agent in Charge to ensure proper compliance. The file review records are subsequently maintained for review by the FBI Inspection Division.

Additionally, all those who approve an undercover operation at the field office level must again review it if it comes up for renewal. For sensitive circumstance-related undercover operations, several FBIHQ units also review the proposal.

In short numerous review processes already exist, and the creation of another entity to perform a review might well be redundant. The FBI, however, will consider whether further reviews of the type recommended might be useful.

The FBI will design a semi-annual inspection tool for use in all undercover operations. Also, the FBI will make available another management tool in the form of a checklist. The FBI will use the checklist every 180 days to manage field undercover operations.

**(13) Establish policies that promote more consistent Division Counsel involvement in the development and implementation of undercover operations, and ensure that Division Counsel are advised of anticipated legal problems in undercover operations.**

**FBI Response**: The FBI concurs with this recommendation. The Chief Division Counsel (CDC) in an FBI Field Office plays an important role in all undercover operations. Based upon present operating standards and existing FBI policy, the CDC's role in the undercover operation is ongoing throughout the undercover operation.

The CDC is regularly consulted by the field office Undercover Coordinator, squad supervisor, and at times, a prospective undercover employee during the formulation of an undercover operation. The CDC also serves as a member of the field office undercover review committee.

The CDC regularly prepares a stand-alone legal analysis of the proposed undercover operation. On sensitive undercover operations, the CDC routinely coordinates with the Office of the General Counsel at FBIHQ. In all undercover operations, the CDC signs the undercover proposal noting his or her review and that the proposal is in compliance with the Attorney General Guidelines and FBI policy. At each six-month interval of the undercover operation, the CDC again reviews and analyzes the operation.

The FBI will add language to Section 10 of the Field Guide that outlines specific responsibilities regarding the CDC in undercover operations.

**(14) Because neither the MIOG nor FBI field guides adequately address the issues below, provide guidance on the following:**

- **the meaning of "sensitive circumstances" relating to "systemic corruption" of governmental functions, and the "significant risk" of violence or physical injury to individuals pursuant to Undercover Guidelines Sections IV.C.2.b & IV.C.2.m, respectively;**

- **how to limit the scope of authorizations for otherwise illegal activity in undercover operations; and**

- **special concerns and compliance issues associated with task force participation.**

**FBI Response**: The FBI concurs with this recommendation as modified for each of the four subsections below but, as a general matter, disputes the premise that existing guidance on these matters is "inadequate."

- **the meaning of "sensitive circumstances" relating to "systemic corruption"**

The Manual of Investigative Operations, Part II, Section 10-11 is the governing administrative document concerning undercover operations. That particular section of MIOG refers to the FGUSO, Section Three, which addresses all of the sensitive circumstances enumerated within the Attorney General Guidelines on Undercover Operations. Specifically, Section 3.2.A of the FGUSO addresses the public corruption sensitive circumstances.

Concerning the "systemic corruption" guidance, the FBI believes that adequate procedural guidance exists to ensure that a rational, sound determination is made as to the existence or absence of systemic corruption. Pursuant to the Guidelines and the FGUSO, the Section Chief, Integrity in Government/Civil Rights Section, CID, has the authority and perspective to determine whether public corruption is systemic in any given case. In addition, the Public Corruption Unit (PCU) at FBI has authored a special instructional document titled Field Guide for Public Corruption Investigations, which provides further guidance to assist in making this determination. Finally, the Undercover and Sensitive Operations Unit works closely with the Public Corruption Unit, the Office of the General Counsel, and the field office in all

undercover operations that involve public corruption to determine the presence or absence of this circumstance on a case-by-case basis.

Nevertheless, the FBI concurs that field offices would be assisted by the addition of language in the Field Guide which better describes and defines “systemic corruption.” Such a definition will be developed by USOU in consultation with the PCU and the Office of the General Counsel and some examples of what constitutes systemic corruption will also be included.

- **the meaning of "significant risk of violence or physical injury"**

The Manual of Investigative Operations, Part II, Section 10-11, is the governing administrative document relative to undercover operations. That particular section of MIOG refers to the FBI's Field Guide on Undercover and Sensitive Operations (FGUSO). Section Three of the FGUSO addresses all of the sensitive circumstances enumerated within the Attorney General Guidelines on Undercover Operations. Specifically, section 3.2.D addresses the safety sensitive circumstance.

Simply defined, a significant risk of violence is a situation where it is more likely than not that violence will occur and that violence is likely to result in seriously bodily injury, or even death. A review of undercover operations has found that no authorized undercover operation has had the occurrence of serious bodily injury or death. The Undercover and Sensitive Operations Unit (USOU), in conjunction with other FBIHQ entities, to include the Office of the General Counsel, undertakes sufficient program management in the area of significant risk of violent or physical injury. Undercover operations, both sensitive and non-sensitive are thoroughly reviewed to ensure that all risks of violence or injury are minimized. Undercover operations often employ additional safeguards that may include operations orders and other checks and balances to ensure safety is paramount, and risk is either reduced or eliminated. With sensitive undercover operation proposals, USOU reviews undercover scenarios that include all potential references to violence. In situations where the absence of violence cannot be ensured, USOU has disapproved of the undercover scenario.

Despite the procedural safeguards, the FBI will add language similar to above to the Field Guide that further explains what

constitutes a significant risk of violence to the extent possible.

- **How to Limit the Scope of authorization for Otherwise Illegal Activity**

The FBI concurs with this recommendation and will add language to its Field Guide that promotes a three-part analysis to determine whether OIA is appropriate: 1) OIA should be the minimum necessary to prove the elements of the offense(s) and consistent with prosecutive guidelines; 2) OIA should, when feasible, reflect realistic limitations; and 3) OIA should, when feasible, be measurable and not open-ended. In addition, a policy of imposing case-specific stipulations by the CUORC will be recommended as circumstances dictate.

- **Guidance on the Special Concerns and Compliance Issues Associated with Task Force Participation in Undercover Operations**

The FBI concurs with this recommendation. USOU has developed guidance, policy and training relative to both FBI and non-FBI participants in undercover operations. With the most recent modification to the Attorney General Guidelines in 2002, USOU requested and received concurrence from the Department of Justice (DOJ) to change the term “undercover agent” to “undercover employee,” the recognition of the fact that other than FBI employees sometimes perform undercover duties.

The FBI then created new policy concerning undercover employees. The policy, enacted in 2002 and enhanced in 2003, is contained the FGUSO, sections 10 and 11.

The standards to participate in undercover operations conducted under the direction and control of the FBI do not differ depending on the organizational affiliation of the undercover employee. The FBI employs three phases to certify all law enforcement persons assigned undercover roles in FBI undercover operations. Phase one includes the collection of various administrative data, Henthorn/Giglio reviews and pending administrative inquiries. Additionally, a non-disclosure agreement and a completed memorandum of understanding are sought from the task force officer and his/her agency. In Phase two, prospective undercover employees must successfully undergo and complete a psychological examination. Lastly, completion of Phase three

certifies the agent or task force officer for use as an undercover employee.

Clear policy, guidance and training are afforded to prospective non-FBI personnel under consideration for use as undercover employees. USOU is aware that compliance with such standards and policies may not be consistent in all FBI field offices. To ensure effective program oversight, USOU thoroughly reviews all sensitive and non-sensitive undercover operations for compliance to the three phases of certification. Additionally, on-site reviews and the inspection process serve as methods to ensure compliance in this area.

To improve program management in undercover operations relative to task force officers, USOU will employ a Task Force Officer review mechanism. The following criteria are for consideration of non-FBI employees in an undercover capacity:

- Complete a required undercover employee consideration checklist
- Obtain a MOU/letter of agreement from the TFO's agency
- Conduct Henthorn/Giglio review
- Conduct pending internal affairs review
- Successfully complete a Safeguard psychological assessment or equivalent
- Complete a TFO non-disclosure form
- Obtain certification from a Special Agent in Charge, pursuant to FGUSO, section 11 or successfully complete the FBI undercover certification course

**(15) Identify ways to enhance Undercover Guidelines compliance training for field supervisors and undercover employees, including use of instructional CD-ROMs, web-based courses, and joint training with the U.S. Attorneys' Offices. Absent exigent circumstances, either as part of the certification of undercover employees or otherwise, the FBI should require undercover employees to complete undercover operation compliance training before participating in undercover operations. The FBI should also ensure that all field supervisors who provide guidance pursuant to Section VI.A of the Guidelines regarding preparation of undercover employees are familiar with undercover techniques, compliance requirements, and the Field Guide for Undercover & Sensitive Operations.**

**FBI Response**: The FBI concurs with this recommendation. The FBI employs sophisticated and advanced undercover training. Many countries have modeled their undercover programs and their undercover training after the FBI. Numerous state, local and federal agencies emulate the FBI's undercover program.

Following the OIG recommendation above, the FBI determined that all members of the undercover review team, with the exception of the field supervisor, receive some type of specialized undercover related training. Undercover employees are trained in backstopping and certified for use in undercover operations. Case agents receive training relative to managing the undercover investigation. Case accountants or financial analysts receive training to ensure their compliance with confidential funding matters. Immediately upon review of the OIG report, the Undercover and Sensitive Operations Unit (USOU) developed a block of instruction for FBI supervisors concerning undercover operations. On 07/19/2005, USOU personnel presented the first block of instruction to about 45 FBI supervisors at the Supervisor's Management Course at the FBI Academy in Quantico, Virginia.

USOU will continue to enhance undercover training for all members of the undercover investigative team using all means possible. Undercover compliance, awareness and certification will be made part of a newly enhanced undercover operation proposal.

**(16) As part of the Undercover Coordinator's certification currently provided for Group I and II undercover operation proposals, add a certification that the instructions set forth in Section VI.A.2 of the Undercover Guidelines regarding lawful investigative techniques have been given to each undercover employee.**

**FBI Response**: The FBI concurs with this recommendation. The Undercover and Sensitive Operations Unit (USOU) will amend the undercover proposal. The amendment will include a certification that the instructions set forth in Section VI.A.2 of the AGG have been given to each undercover employee. The new undercover proposal includes a section where all members of the undercover investigative team certify their review of the AGG.

**(17) Amend the Group I and Group II undercover operation proposals forms that currently provide information regarding**

**the expected execution of the undercover operation to include a section: "Facts Pertinent to Violence Risk Assessment."**

**FBI Response**: The FBI concurs with this recommendation. The Undercover and Sensitive Operations Unit (USOU) will amend the undercover proposal. The amendment will include a section titled "Facts Pertinent to Violence Risk Assessment." USOU will provide field guidance about the information required in this new section of the undercover proposal.

**(18) Require field offices seeking approval of Group 1 undercover operations to obtain concurrence letters from U.S. Attorneys' Offices that meet the requirements of Section IV.F.2.b of the Undercover Guidelines and amend Section 4.8(5) of the Field Guide for Undercover & Sensitive Operations accordingly.**

**FBI Response**: The FBI concurs with this recommendation. The Undercover and Sensitive Operations Unit (USOU) will be responsible to ensure full compliance of Section IV.F.2.b of the Attorney General Guidelines on Undercover Operations. Specifically, USOU will ensure that the letter received from the respective United States Attorney's Office (USAO) is signed by the United States Attorney (USA), or the applicable official who is acting in that capacity at the time the letter is authored.

Additionally, USOU will ensure that all USAO letters associated with Group I UCO submissions contain the following language:

- the USAO has reviewed the proposed operation, including any sensitive circumstances reasonably expected to occur
- the USAO agrees with the proposal and its legality
- the USAO finds that the proposed investigation would be an appropriate use of the undercover technique
- the USAO believes that the potential benefits in detecting, preventing, or prosecuting criminal activity outweigh any direct costs or risks of other harm
- the USAO will prosecute any meritorious case that is developed.

**(19) Ensure that the Undercover and Sensitive Operations Unit has access to the Inspection Division's undercover operation audits.**

**FBI Response**: The FBI concurs with this recommendation. The Undercover and Sensitive Operations Unit (USOU) Chief has already coordinated this matter with an Assistant Inspector of the Inspection Division (INSD). USOU and INSD have reviewed inspection-related criteria associated with the FBI's undercover programs and made changes resulting in a more effective and efficient review of the undercover program during the inspection process. For example, INSD now grants USOU access to its undercover operation audits.

**(20) Ensure compliance with the General Crime Guidelines' requirements to obtain and document authorizations for the extension, conversion to full investigation, and closing of preliminary inquiries.**

**FBI Response**: The FBI concurs with this recommendation. The FBI will ensure compliance with the General Crimes Guidelines' requirements to obtain and document authorizations for the extension, conversion to full investigation, and closing of preliminary inquiries.

**(21) Institute measures to ensure consistency in meeting and documenting the notification and reporting requirements provided in Sections III.A.5 and III.B.4 of the General Crimes Guidelines, including requiring FBI field offices to maintain in the relevant investigative file documentation of the notice of the opening of criminal intelligence investigations to DOJ's Counterterrorism, Organized Crime and Racketeering Sections, Office of Intelligence Policy and Review (OIPR), and the relevant U.S. Attorneys' Offices as required in racketeering enterprise investigations and terrorism enterprise investigations. The FBI should also ensure that progress reports required by the Guidelines in terrorism enterprise investigations are provided to OIPR, DOJ's Counterterrorism Section, and FBI Headquarters.**

**FBI Response**: The FBI concurs with this recommendation with the exception discussed below. The Criminal Investigative Division, Criminal Intelligence Section, Criminal Intelligence Management & Policy Unit (CIMPU) was established in March 2003. The CIMPU recognized that the FBI had a problem with consistency in meeting and documenting the notification and reporting requirements in III.A.5 and III.B.4 of the General

Crimes Guidelines, and immediately took steps to develop and institute policy and procedures to remedy this problem. Within three months, by electronic communication (EC) to all field offices, dated 06/23/2003, entitled "Racketeering Enterprise Investigations (REI)", the CIMPU reiterated FBI policy and procedures for uploading all communications in an REI and for meeting and documenting the notification and reporting requirements provided in III.A.5 and III.B.4 of the General Crimes Guidelines.

All field offices were specifically advised of the policy and procedures necessary to comply with AG and FBI Guidelines for REIs and the necessity of advising CIMPU of the initiation of all REIs. CIMPU advised the field that upon notification of an REI, CIMPU would review the file for compliance issues and upon ensuring the file was in compliance, notify DOJ OCRS of the initiation of the REI and document that in the field office REI file, both electronically in the FBI's Automated Case Support (ACS) system and by hard copy mailed to the field office.
As part of its compliance review, upon notification of the initiation of an REI by the field office, CIMPU will also institute a check to ensure the field office has notified the appropriate U.S. Attorneys' Office.

With respect to terrorism enterprise investigations (TEI), the Domestic Terrorism Operations Section (DTOS) meets regularly with counterparts in the Counterterrorism Section at DOJ to brief them on the openings, progress, and renewals of these investigations. DTOS will take measures to ensure that compliance with the Guidelines notice requirements are consistently documented in field office case files. In addition, although the General Crimes Guidelines envision that the TEI will be used to gather criminal intelligence in international terrorism cases, the Counterterrorism Division made the policy decision to restrict the TEI to domestic terrorism only and to collect intelligence on and investigate international terrorism matters under the National Security Investigative Guidelines rather than the General Crimes Guidelines. For this reason, notice to OIPR of TEI openings, progress, and renewals is not made as domestic terrorism is not within OIPR's charter. If this policy is changed to open TEIs on international terrorism, notice to OIPR of those cases will be made as a matter of course.

**(22) Discuss with DOJ how to reconcile Section 100-2.3(3) of the MIOG, requiring Headquarters' concurrence the initiation**

**and renewal of terrorism enterprise investigations, with Sections III.B.4.a & b of the General Crimes Guidelines, which authorize field level initiation and renewal of these investigations.**

**FBI Response:** The FBI concurs with the recommendation that reconciliation between the Guideline authority for field office approval of TEIs and the MIOG requirement for HQ approval should be discussed with DOJ. The Counterterrorism Division, however, requires FBIHQ concurrence of SAC authorization to initiate and renew a TEI to ensure centralized program management of these investigations, which typically involve groups with a nation-wide presence, and to permit higher level review of these sensitive investigations that usually implicate first amendment concerns. Although it is the FBI's position that these reasons for the variance from the Guidelines authority are valid, this matter will be discussed with DOJ and appropriate reconciliation pursued.

**(23) Require field level supervisory approval prior to the exercise of Part VI.A.2 authorities to visit public places or attend public events for the purpose of detecting or preventing terrorist activities, absent exigent circumstances.**

**FBI Response:** The FBI concurs with this recommendation. The Counterterrorism Division will send a communication to all field offices setting forth this policy.

**(24) Develop a standardized form or a short e-mail template to be completed by case agents to document their use of the Part VI.A.2 authorities.**

**FBI Response:** The FBI concurs with this recommendation. The Counterterrorism Division will request that this statistic be captured under the re-engineering process currently underway.

**(25) In light of the survey responses of Division Counsel, consider whether (a) field office practices since May 30, 2002, regarding predication, collection, record retention, indexing, and dissemination of Part VI.A information, and the practices regarding utilization of "zero files" or other files to capture Part VI.A information, are in conformity with the Guidelines and FBI guidance; (b) there is a need for further guidance on predication, collection, record retention, indexing, dissemination, or other issues; and (c) FBI Headquarters managers should have access to data reflecting**

**use of Part VI.A.2 authorities in order to be satisfied that these authorities are used in conformity with the Guidelines.**

**FBI Response:** The FBI concurs with the recommendation to consider the three matters listed above. The Counterterrorism Division will consult with the Office of the General Counsel to review existing guidance and to determine whether additional guidance concerning the collection, retention, and dissemination of Part VI.A.2 information is required and, if so, how to make those data available to HQ program managers.

**(26) Ensure that required authorizations for consensual monitoring are obtained in advance and are appropriately documented.**

**FBI Response**: The FBI concurs with this recommendation and will ensure that required authorizations for consensual monitoring are obtained in advance and are appropriately documented.

**27) For monitorings that do not require DOJ approval, consult with DOJ to resolve whether the Consensual Monitoring Guidelines should be interpreted to authorize monitoring for more than 90 days (including up to "the duration of the investigation" as currently provided on Form FD-759), or whether the authorization is limited to 90 days. The resulting interpretation should be incorporated in the FBI's MIOG and communicated to the field.**

**FBI Response**: The FBI concurs with the recommendation. By letter dated August 25, 2005, the Director of DOJ, Office of Enforcement Operations (OEO), advised that the Consensual Monitoring Guidelines should be interpreted to authorize monitoring for more than 90 days (including up to “the duration of the investigation” as currently provided on Form FD-759). The FBI is also evaluating OEO’s response to determine if any further clarification of current FBI policy is advisable.

**(28) Provide CUORC members, upon request, with access to copies of Inspection reports concerning undercover operations, the Undercover and Sensitive Operations Unit on-site reviews, and after-action reports of undercover operations.**

**FBI Response**: The FBI concurs with this recommendation. The Undercover and Sensitive Operations Unit (USOU) Chief has already coordinated this matter with an Assistant Inspector of

the Inspection Division (INSD). USOU and INSD have reviewed inspection-related criteria associated with the FBI's undercover programs and already effected modifications to enhance a more effective and efficient review of the undercover program during the inspection process. The INSD has agreed to permit the USOU access to the INSD's undercover operation audits.

**(29) Consider ways for the Undercover and Sensitive Operations Unit to develop more complete information for the CUORC and other FBI components, such as conducting a periodic analysis of the patterns and trends found in its on-site reports, informing the CUORC members of any persistent Guidelines violations, and providing copies of its semi-annual report to all FBI Headquarters operating Divisions, the Office of General Counsel, and the Training Division.**

**FBI Response**: The FBI concurs with this recommendation. The Undercover and Sensitive Operations Unit (USOU) enjoys a positive relationship with the members of the Criminal Undercover Operations Review Committee (CUORC). As noted in OIG recommendation 28, the AGG, Section D, defines the role and responsibility of the CUORC. Since its inception, the CUORC has ensured the FBI's proper application of the undercover technique in a variety of investigative and intelligence matters.

The FBI vigorously reviews the conduct of its undercover personnel and undercover operations. Any inconsistencies with the AGG or FBI undercover policy are brought forthwith to the CUORC.

The FBI's semiannual report is maintained in accordance with all applicable records management policies. As such, appropriate entities inside and outside the FBI can conduct an appropriate review of the report(s) as needed.

**(30) To assist CIRC members in evaluating the confidential informants within its purview and assist field and Headquarters managers in their supervisory responsibilities in overseeing the Criminal Informant Program, require that the Initial and Continuing Suitability Reports and Recommendations contain more thorough answers to the suitability questions, such as:**

**• A description of the legitimate source of income of confidential informants.**

**• The confidential informants' statistical accomplishments, including the number of indictments, convictions, Title III wiretap applications, and other indicia of the informant's contributions.**

**• Details on how confidential informants are in a position to obtain relevant information.**

**• Details on the nature of any unauthorized illegal activity committed by confidential informants, including the informants' criminal history record and the continuing suitability reports required to be completed in accordance with Section II.A.2.b of the Confidential Informant Guidelines.**

**• The informant record of any confidential informant who was previously deactivated for cause by the FBI, including the reasons for deactivation and the field division operating the informant.**

**FBI Response**: The FBI concurs with this recommendation. The Directorate of Intelligence will amend the SR&R forms to prompt agents to provide more thorough answers to suitability questions. In the CIRC context, the thorough responses will allow DOJ attorneys to concentrate on decision-making rather than fact-finding.

**(31) Consider having the Human Intelligence Unit draft "lessons learned" from the CIRC's decisions, periodically communicate these lessons to field personnel, and incorporate them into training on the Confidential Informant Guidelines.**

**FBI Response**: The FBI concurs with this recommendation. When resources are available, “lessons learned” from the CIRC’s decisions will be drafted and disseminated to field office personnel monthly through an electronic communication or the Intranet web page. These lessons will be incorporated into training on the Confidential Informant Guidelines.

**(32) Make available to CIRC members, upon request, copies of the Inspection Division's audits of the Criminal Informant Program (including any reinspection reports) and evaluations performed by the Human Intelligence Unit of compliance with the Confidential Informant Guidelines.**

**FBI Response**: The FBI concurs with this recommendation. The FBI will consider any requests from CIRC members for

Inspection Division audits of the Confidential Informant Program, re-inspection reports concerning human sources, and HIU evaluations. However, we believe that generally it is not necessary for the DOJ to receive this information in order to carry out the essential purpose of the CIRC.

**(33) Revise Inspection Division checklists and interrogatories to increase inspection coverage of Guidelines-related issues.**

**FBI Response**: The FBI concurs with this recommendation. In July 2005, the INSD revised informant program checklists to include all matters recommended by the OIG, and increased inspection coverage of guidelines-related issues. The revised checklist questions cover all AGG issues related to the operation of criminal informants.

**(34) As part of the Inspection Division's triennial inspections of field and Headquarters' divisions, establish an audit examining the collection of information obtained from exercise of counterterrorism authorities pursuant to Section VI.A.2 (Visiting Public Places and Events) of the General Crimes Guidelines.**

**FBI Response**: The FBI concurs with this recommendation.

**(35) Provide more thorough and timely reporting of Guidelines violations by identifying in inspection reports the causes and gravity of compliance deficiencies; developing summary statistics to assist in determining when reinspections are appropriate; and automating key components of the inspection process.**

**FBI Response**: The FBI concurs with this recommendation. It should be noted the INSD Criminal Informant Program (CIP) checklists have been revised to collect information on the causes of identified deficiencies. In addition, the INSD is in the process of creating a computer database to assist in analyzing the results of compliance audits.

**(36) Increase inspections for the Criminal Informant Program and other programs that are priorities or experiencing significant problems by performing more frequent inspections at irregular times. The Inspection Division should also develop a standard for reinspections that accounts for the frequency and seriousness of the Guidelines deficiencies identified during the regular inspection and develop a**

**standard for determining when reinspections should be conducted that accounts for both the number and gravity of the deficiencies found. The Inspection Division and the Human Intelligence Unit should reinstate its Criminal Informant Program reinspection process.**

**FBI Response**: The FBI concurs with this recommendation.

**(37) Address in employee performance appraisals the findings from Inspection Division inspections that identify either superior or deficient Guidelines compliance performance.**

**FBI Response**: The FBI concurs with this recommendation to address this element of performance in employee performance appraisals and will explore ways to accomplish this goal within the limits of the regulations that govern this process as well as the limitations of the FBI Performance Appraisal System.

**(38) Elevate egregious non-compliance with Guidelines to an executive management finding in the inspection report rather than deferring that action until the next three-year inspection contingent on the detection of recurring, serious deficiencies.**

**FBI Response**: The FBI concurs with this recommendation.

**(39) The Inspection Division and the Human Intelligence Unit should institute procedures that establish follow-up inspection measures to reinspections that indicate on-going compliance problems, such as assigning a single Assistant Inspector in Place to conduct an additional inspection within the first six months following the reinspection.**

**FBI Response**: The FBI concurs with this recommendation.

**(40) Modify the Undercover and Sensitive Operations Unit on-site review data collection instrument to better address Guidelines compliance, including issues such as otherwise illegal activity, potential entrapment issues, and task force participation.**

**FBI Response**: The FBI concurs with this recommendation.

**(41) Ensure that Attorney General Guidelines violations warranting potential discipline are referred to the FBI's**

**Internal Investigations Section in a consistent fashion throughout the FBI.**

**FBI Response:** The FBI concurs with this recommendation.

**(42) Ensure that the Inspection Division's standards for referring misconduct involving Guidelines violations are consistent with practices adopted by the Internal Investigations Section.**

**FBI Response:** The FBI concurs with this recommendation and a new process has already been implemented by the INSD.

**(43) Add separate offense codes for: (i) knowingly or recklessly failing to obtain proper authorization for a source's participation in otherwise illegal activity; (ii) knowingly or recklessly failing to obtain proper authorization to operate long-term, high level, privileged or media-affiliated confidential informants or other informants subject to special approval requirements; and (iii) knowingly or recklessly failing to operate long-term, high level, privileged or media-affiliated confidential informants, or other informants subject to special approval requirements in accordance with the relevant Confidential Informant Guidelines and MIOG provisions.**

**FBI Response**: The FBI concurs with this recommendation. A team from the INSD and the Office of Professional Responsibility has been formed to ensure that the three new offense codes are added in accordance with the relevant Confidential Informant Guidelines and MIOG provisions.

**(44) Assign some person or unit at FBI Headquarters the responsibility to develop a plan to ensure proper and timely execution of the revisions and to coordinate implementation of the revisions over time.**

**FBI Response**: The FBI concurs with this recommendation and will determine the best way to implement it.

**(45) Distribute the revised Guidelines to Chief Division Counsel, together with a concise summary or listing of the changes, sufficiently in advance of the new Guidelines' effective date to allow field personnel to familiarize themselves with the revisions and to allow those Headquarters and field personnel who provide training on the revisions to develop training materials and a schedule for providing**

**training. In addition, near the effective date of the revision, the FBI should develop and distribute standardized forms and other administrative support tools, issue field guidance, and identify a Headquarters point of contact who can address questions concerning the revisions.**

**FBI Response**: The FBI concurs with this recommendation.

**(46) Ensure that revisions to the MIOG accurately reflect any changes to the Guidelines and are made on or about the effective date of such changes.**

**FBI Response**: The FBI concurs with this recommendation with the reservation that if a considered agency decision is made to impose more restrictive procedural requirements in the MIOG for agency oversight purposes than those required by the Guidelines, then such distinctions and the reasons therefore be documented and explained in the MIOG revisions.

**(47) Make appropriate changes to the MIOG to reconcile the discrepancies between the Guidelines and the MIOG that are identified in this report.**

**FBI Response**: The FBI concurs with this recommendation that appropriate changes to the MIOG should be made where true discrepancies exist. Furthermore, the responsibility for making the MIOG changes should be assigned to the FBI HQ entity that disseminated the field wide guidance on the 2002 revisions.

# APPENDIX H

# OIG ANALYSIS OF THE FBI RESPONSE TO OIG RECOMMENDATIONS

In accordance with the OIG's standard procedures, the OIG provided a draft of this report to the FBI on July 12, 2005, for its review. The FBI comments to the draft report are provided in Appendix G. In its response, the FBI concurred with 43 of the 47 recommendations and concurred with the remaining 4 recommendations, with modifications. In many of the responses, the FBI provided a description of actions or procedures it has recently implemented or proposes to implement in response to our recommendations. We are asking the FBI to provide to us, when they are implemented, a description of these actions and procedures. When we receive this material, the OIG will examine whether the FBI's actions address our recommendations and whether those recommendations should be closed.

Our analysis of the FBI's comments on each recommendation follows.

**Recommendation Number:**

1. **Resolved.** In response to this recommendation to develop a compliance plan for the FBI's human source program and an implementation plan to put the plan into practice, the FBI stated that it concurs with this recommendation. The FBI stated that its Directorate of Intelligence is re-engineering the Human Source Program with emphasis on improving compliance with the Attorney General's Guidelines and FBI policy. The FBI described the elements of its re-engineering efforts, which include new guidelines, policies, manuals, technologies, training initiatives, and processes for the utilization of human sources.

As this review was completed, the FBI had not yet finalized the various elements of its re-engineering initiative, and no new Guidelines or Guidelines interpretations have been issued. Please provide us the approved re-engineering plan when it is completed, as well as the compliance and implementation plans called for in the recommendation.

2. **Resolved.** In response to this recommendation to develop standardized forms to capture the most significant Attorney General Guidelines and MIOG requirements for operating confidential informants, a standardized file review "cover sheet," and an electronic user's manual, the FBI stated that it concurs with this recommendation. The FBI stated that standardized forms and file review cover sheets are a major component of the re-engineering initiatives for the Human Source Program and that the automation component of that initiative will have "built-in features that

prevent users from proceeding without completing critical areas of the template . . ." In addition, because the FBI does not anticipate that the initial aspects of the initiative will be implemented until January 2006, the FBI stated that it will consider creating and implementing stop-gap uniform standardized forms throughout the FBI.

Please provides us with the approved re-engineering plan, including plans for standardized electronic forms, file review "cover sheets," and a user's manual to be used throughout the FBI, together with guidance and notifications necessary to implement the changes. In addition, if the FBI decides to provide stop gap standardized forms until the reengineering initiatives are in place, please provide us with the standardized forms and any other interim measures to address this recommendation on an interim basis.

3. **Resolved.** In response to this recommendation that the FBI institute procedures for determining if state or local prosecuting offices have filed charges against confidential informants who engage in "unauthorized illegal activity (OIA)," the FBI stated that it concurs with this recommendation. The FBI stated that case agents who handle CIs are responsible for determining whether a state or local prosecutor has filed charges against the CI and that first-line supervisors are responsible for ensuring that that the Chief Federal Prosecutor is notified if a CI engages in unauthorized illegal activity. However, the FBI acknowledged that a field office's ability to learn of unauthorized activity by its CIs varies widely among local law enforcement agencies. The FBI stated that the Directorate of Intelligence will consider designing a standard 90-day file review format (and related manual revisions and re-engineering efforts) which will prompt the first-line supervisor to ensure that relevant documentation is contained in the CI's file.

Please provide a description of the new procedures, together with any guidance or notifications necessary to implement this recommendation.

4. **Resolved.** In response to this recommendation to amend forms used to authorize "otherwise illegal activity" so as to assist case agents in distinguishing Tier 1 "otherwise illegal activity" from Tier 2 "otherwise illegal activity," the FBI stated that it concurs with this recommendation. The FBI stated that implementing Bureau-wide standardized forms that include the definitions of Tier 1 and Tier 2 OIA and prompt agents to provide specific information about the anticipated "otherwise illegal activity" in which the CI is authorized to participate will provide useful guidance for agents and supervisors. However, the FBI notes that because the U.S. Sentencing Guidelines information may be too voluminous to include in a standardized form, this information will be accessible through the Human Intelligence

Unit's Intranet web page and links to the proposed automated re-engineering system.

Please provide us with the standardized forms and related manual revisions, together with any guidance or notifications necessary to implement this recommendation, and describe the pertinent re-engineering efforts.

5. **Unresolved.** In response to this recommendation to revise the FBI's promotion policies and the performance plans for Special Agents and executive managers to indicate, where applicable, that compliance or overseeing compliance with the Confidential Informant Guidelines will be considered in employees' annual performance appraisals, the FBI stated that it concurs with the recommendation. However, the FBI stated that it believes the current mandatory element sufficiently addresses Section I.I of the Confidential Informant Guidelines' requirement because the referenced element contains a reference to "all applicable AG Guidelines."

We do not believe the FBI's current performance plans comply with Section I.I of the Confidential Informant Guidelines. Prior to the May 2002 revisions of the CI Guidelines, which require that compliance with the CI Guidelines be explicitly referenced in performance plans, there was a generic reference in the critical elements for Special Agents GS 10 to GS 14 and for GS 15 and Senior Level Special Agents to "make decisions in accordance with existing policies and procedures (e.g., follows Attorney General guidelines)." The critical element for these agents in the forms effective during the period prior to the most recent revision contained the same generic reference. Accordingly, we believe that the Guidelines' revision issued in January 2001 to make explicit reference to the Confidential Informant Guidelines was intentional and that the generic reference in the performance plans effective April 2005 does not comply with the spirit or the letter of the revisions to the Guidelines.

In its response to this recommendation, the FBI also did not address parallel changes the OIG recommends for referencing compliance and overseeing compliance with the CI Guidelines in FBI promotion policies.

Accordingly, this recommendation remains unresolved. The FBI may resolve this recommendation by revising its performance plans for all Special Agents and executive managers to indicate that compliance or overseeing compliance with the Confidential Informant Guidelines will be considered in employees' annual performance appraisals, and making corresponding revisions to its promotion policies.

6. **Resolved.** In response to this recommendation that the FBI evaluate the grade level of Special Agents who serve as Confidential Informant

Coordinators and consider allowing Confidential Informant Coordinators to be elevated to a GS-14 supervisory level, particularly in larger FBI field offices, the FBI stated that it concurs with this recommendation.

Accordingly, please provide us with the results of the FBI's review and analysis.

7. **Resolved.** In response to this recommendation that the FBI consider holding annual Informant Coordinator Conferences as well as opportunities for local, joint training with representatives from the U.S. Attorney's Offices on certain topics (such as Guidelines' provisions requiring approval, concurrence or notice to the U.S. Attorney's Offices; the harm of Guidelines' violations from the standpoint of the prosecution and the FBI; and "lessons learned" from past cases), the FBI stated that it concurs with this recommendation.

Accordingly, please provide us with the results of the FBI's consideration of holding annual Informant Coordinator Conferences as well as the other joint training programs and topics referenced in our recommendation.

8. **Resolved.** In response to this recommendation that the FBI review the training modules now used in New Agent training, probationary training, and in-service training for Special Agents and Supervisory Special Agents to ensure that key Confidential Informant Guidelines' requirements and risks of operating informants are explained, the FBI stated that it concurs with this recommendation. The FBI also stated that the Human Intelligence Unit and the Training Division are updating training modules in conjunction with the re-engineering initiatives and, in the interim, will ensure that current Guidelines' requirements and risks of operating CIs are fully explained.

Accordingly, please provide us with the current training modules; any interim, updated training modules used pending completion of the Human Source re-engineering initiatives; and the training modules developed as part of those initiatives.

9. **Resolved.** In response to this recommendation to include in the periodic training of Supervisory Special Agents a component or module on the importance of file reviews to the Criminal Informant Program and frequently occurring Guidelines and MIOG violations with the objective of stressing predictors of problems with confidential informants, the FBI stated that it concurs with this recommendation and has begun implementation. The FBI stated that the Directorate of Intelligence has provided specific guidance for conducting human source file reviews to Headquarters Supervisory Special Agents who are en route to field supervisory positions,

with emphasis on recurring Guidelines and MIOG violations, and that regular training and training materials will be made available to field office supervisory personnel in the future.

Accordingly, please provide us with details of the new training modules and other aspects of the training component of the re-engineering initiative.

10. **Resolved.** In response to this recommendation that the FBI evaluate the grade level of Special Agents who serve as Undercover Coordinators and consider allowing Undercover Coordinators to be elevated to a GS-14 supervisory level, the FBI stated that it concurs with this recommendation. In addition, the FBI stated that it may, if feasible, direct a study to determine whether the duties and responsibilities of the Undercover Coordinators are commensurate with a grade change to a GS-14. The FBI also stated that it will advise Special Agents in Charge to assign GS-14 supervisors collateral duties as Undercover Coordinators, resulting in changes in 16 of the FBI's 56 field offices.

Accordingly, please provide the referenced study and the results of the FBI's analysis.

11. **Resolved.** In response to this recommendation that the FBI encourage regular consultation between members of its undercover investigative teams and Undercover Coordinators during the formulation and conduct of undercover operations, the FBI stated that it concurs with this recommendation. The FBI also stated that it will add language to the USOU's Field Guide for Undercover and Sensitive Operations outlining responsibilities of the Undercover Coordinator, including the duty to regularly consult with undercover teams, and will ensure such consultations continue through training, undercover reviews, and executive level briefings.

Accordingly, please provide details of the revised Field Guide provisions and other measures the FBI has agreed to undertake.

12. **Resolved.** In response to this recommendation that the FBI evaluate ways for Undercover Coordinators to perform progress reviews at least every 90 days on undercover operations, a component of which should include an evaluation by senior managers, in consultation with Division Counsel and the Undercover Coordinator, of compliance with the Undercover Guidelines, the FBI stated that it concurs with the recommendation, with modification. The FBI noted that 90-day file reviews are already conducted by supervisors and are reviewed by an Assistant Special Agent in Charge "to ensure proper compliance," and that undercover operation proposals involving "sensitive circumstances" are reviewed by several Headquarters' units.

The FBI stated that in lieu of a 90-day progress review or progress reviews conducted by Undercover Coordinators, it will design a semi-annual inspection tool for use in all undercover operations and will make available a checklist to assist FBI managers in managing field undercover operations. The FBI stated that it believes that these measures, in conjunction with existing review processes at the field and Headquarters level, are sufficient to ensure compliance with the Undercover Guidelines. The FBI's response did not, however, indicate what steps it has taken or will take to ensure that Undercover Coordinators and Division Counsel are consulted in the course of the progress reviews.

Accordingly, while we believe the FBI's response addresses the intent of our recommendation, it does not fully address our recommendation. Please provide details of the FBI's planned semi-annual inspection tool, new checklist, and efforts to ensure that Undercover Coordinators and Division Counsel are consulted in the course of the progress reviews.

13. **Resolved.** In response to this recommendation that the FBI establish policies that promote more consistent Division Counsel involvement in the development and implementation of undercover operations and ensure that Division Counsel are advised of anticipated legal problems in undercover operations, the FBI stated that it concurs with the recommendation. The FBI stated that it will add language to Section 10 of the Field Guide for Undercover and Sensitive Operations that outlines specific responsibilities of the Chief Division Counsel in undercover operations. The FBI did not, however, indicate how it intended to reinforce the role of Division Counsel other than Chief Division Counsel in undercover operations in its communications and guidance to Division Counsel and in periodic training of Division Counsel. In view of the fact that not all Chief Division Counsel will be in a position to become involved in all significant developments involving undercover operations, we believe the measures undertaken in response to this recommendation, including guidance and training, be directed to all Division Counsel.

Accordingly, please provide the revised Field Guide provisions and indicate how the FBI intends to promote consistent Division Counsel involvement in the development and implementation of undercover operations.

14. **Resolved.** In response to this recommendation that the FBI revise portions of the MIOG and the Field Guide for Undercover and Sensitive Operations to provide guidance on the meaning of four key phrases in the Undercover Guidelines applicable to undercover operations, the FBI stated that it concurs with the recommendation, with modification. As a general

matter, the FBI disputed the premise that its existing guidance is "inadequate."

a. The meaning of "sensitive circumstances" relating to "systemic corruption" of government functions

With respect to the meaning of the phrase, "sensitive circumstances" relating to "systemic corruption" of governmental functions, the FBI stated that there is adequate procedural guidance to ensure that a "rational, sound determination is made as to the existence or absence of systemic corruption." The FBI further stated that the its Public Corruption Unit has authored special guidance and that the unit works closely with the Undercover and Sensitive Operations Unit and the Office of the General Counsel to determine whether such circumstances exist. The FBI stated that field offices would nonetheless be assisted by Field Guide revisions that better describe and define "systemic corruption," and that this material will be developed by the Undercover and Sensitive Operations Unit in consultation with the Public Corruption Unit and the Office of the General Counsel.

b. The meaning of "significant risk" of violence or physical injury to individuals

With respect to the meaning of the phrase "significant risk" of violence or physical injury to individuals, the FBI stated that a "significant risk of violence" is a situation where "it is more likely than not that violence will occur and that violence is likely to result in serious[ly] bodily injury or even death." The FBI further stated that a review of undercover operations has found that no authorized undercover operation has had the occurrence of serious bodily injury or death and that risks of violence or physical injury are minimized. The FBI noted that in situations where the absence of violence cannot be ensured, the Undercover and Sensitive Operations Unit has disapproved the proposal. The FBI stated that, despite existing procedural safeguards, it will add language to the Field Guide that further explains what constitutes a significant risk of violence to the extent possible.

c. How to limit the scope of authorizations for "otherwise illegal activity" in undercover operations

With respect to "otherwise illegal activity" during undercover operations, the FBI stated that it will add language to its Field Guide for Undercover and Sensitive Operations that promotes a three-part analysis to determine whether "otherwise illegal activity" is appropriate and recommend a policy imposing case-specific stipulations by the CUORC as circumstances dictate.

d. Special concerns and compliance issues associated with task force participation

With respect to special concerns associated with task force participation in undercover operations, the FBI stated that the Field Guide for Undercover and Sensitive Operations contains guidance concerning undercover employees and that the standards to participate in undercover operations conducted under the direction of the FBI do not differ depending on the organizational affiliation of the undercover employee. The FBI stated that clear policy, guidance, and training are afforded to non-FBI personnel under consideration for use as undercover employees. The FBI acknowledged, however, that compliance with such standards and policies "may not be consistent in all FBI field offices," but that the Undercover and Sensitive Operations Unit "thoroughly reviews all sensitive and non-sensitive undercover operations for compliance to the three phases of certification." The FBI stated that in order to improve program management of undercover operations relative to task force officers, the Undercover and Sensitive Operations Unit will employ a Task Force Officer review mechanism which will employ specified compliance criteria.

Accordingly, with respect to all four issues, please provide the new definitions and Field Guide revisions, and details of the Task Force Officer review mechanism.

15. **Resolved.** In response to this recommendation that the FBI identify ways to enhance Undercover Guidelines compliance training for field supervisors and undercover employees, the FBI stated that it concurs with the recommendation. The FBI acknowledged that while other members of its undercover review teams receive some type of specialized undercover-related training, field supervisors do not receive such training. The FBI noted that undercover employees, case accountants, and financial analysts receive certain types of training, but did not indicate whether their training is relevant to Guidelines compliance. The FBI stated that upon receipt of the OIG draft report, the Undercover and Sensitive Operations Unit has developed a block of instruction for FBI supervisors and that it completed the first block of instruction to about 45 supervisors at the Supervisor's Management Course held on July 19, 2005.

Accordingly, please provide details of the new training for FBI supervisors and enhanced training measures for undercover employees.

16. **Resolved.** In response to this recommendation that the FBI add a certification as part of the Undercover Coordinator's certification for Group I and Group II undercover operations proposals, to the effect that the instructions set forth in Section VI.A.2 of the Undercover Guidelines

regarding lawful investigative techniques have been given to each undercover employee, the FBI stated that it concurs with the recommendation and will amend the undercover proposal form and the pertinent certification.

Accordingly, please provide the revised proposal form and certification for Group I and Group II undercover operations proposals, together with any guidance and notifications necessary to implement this recommendation.

17. **Resolved.** In response to this recommendation that the FBI amend its Group I and Group II undercover proposal forms to include a section titled, "Facts Pertinent to Violence Risk Assessment," the FBI stated that it concurs with the recommendation and will amend the undercover proposal form.

Accordingly, please provide the revised undercover proposal form, together with any guidance and notifications necessary to implement this recommendation.

18. **Resolved.** In response to this recommendation that the FBI require field offices seeking approval of Group I undercover operations to obtain concurrence letters from U.S. Attorneys' Offices that meet the requirements of Section IV.F.2.b of the Undercover Guidelines and make corresponding changes to Section 4.8(5) of the Field Guide for Undercover and Sensitive Operations, the FBI stated that it concurs with the recommendation.

Accordingly, please provide copies of the revised portion of the Field Guide for Undercover and Sensitive Operations, together with any guidance and notifications necessary to implement this recommendation.

19. **Resolved.** In response to this recommendation that the FBI ensure that the Undercover and Sensitive Operations Unit have access to the Inspection Division's undercover operations audits, the FBI stated that it concurs with the recommendation.

Accordingly, please provide the notifications necessary to implement this recommendation.

20. **Resolved.** In response to this recommendation that the FBI ensure compliance with the General Crimes Guidelines' requirements to obtain authorizations for the extension, conversion to full investigation, and closing of preliminary inquiries, and maintain appropriate documentation, the FBI stated that it concurs with the recommendation.

Accordingly, please describe how the FBI intends to ensure compliance with the General Crimes Guidelines' requirements to obtain

authorizations for extensions and conversions to full investigation, and maintain appropriate documentation, together with any guidance and notifications necessary to implement this recommendation.

21. **Unresolved.** In response to this recommendation that the FBI institute measures to ensure consistency in meeting and documenting the notification and reporting requirements provided in Sections III.A.5 and III.B.4 of the General Crimes Guidelines and ensure that progress reports required by the Guidelines in terrorism enterprise investigations are provided to OIPR, DOJ's Counterterrorism Division, and FBI Headquarters, the FBI stated that it concurs with the recommendation, with one exception. The FBI stated that in March 2003 it established the Criminal Intelligence Management & Policy Unit (CIMPU) in the Criminal Intelligence Section of the Criminal Investigative Division. According to the FBI, CIMPU took steps to develop and institute policies and procedures to remedy the notification and reporting problems regarding racketeering enterprise investigations. The FBI stated that an electronic communication (EC) dated June 23, 2003, was sent to all field offices noting current policy. With respect to terrorism enterprise investigations, the FBI stated that the Domestic Terrorism Operations Section meets regularly with counterparts in the Counterterrorism Section of the DOJ Criminal Division to brief them on the initiation, progress, and renewals of these investigations and will take further steps to ensure that compliance with the Guidelines requirements are consistently documented in field office case files.

In the course of our field work during this review, we identified at least four racketeering enterprise investigation files involving investigations initiated after the June 23, 2003, EC was sent to the FBI's field divisions that did not contain the required notifications. Accordingly, we continue to have concerns about the adequacy of the steps taken by the FBI to ensure compliance with these Guidelines requirements. We believe that the FBI has not taken steps necessary to ensure that notification and reporting requirements provided in Sections III.A.5 and III.B.4 of the General Crimes Guidelines are satisfied and appropriately documented. Therefore, this recommendation can be resolved when the FBI demonstrates that it has instituted appropriate steps to ensure that the notification and reporting requirements for criminal intelligence investigations are satisfied and appropriately documented.

The exception noted in the FBI's response concerns whether the FBI must notify the OIPR of the initiation and renewal of terrorism enterprise investigations. According to the FBI, following issuance of the May 2002 Attorney General Guidelines, the FBI's Counterterrorism Division made a policy decision to restrict the use of terrorism enterprise investigations to domestic terrorism matters. Therefore, it reasons that because "domestic terrorism is not within OIPR's charter," notice to OIPR is not made. When

the OIG asked OIPR whether it was aware of the FBI's interpretation and practice, OIPR stated that it was not aware of these changes until they were brought to its attention by the OIG. Moreover, an OIPR official noted that 28 U.S.C. § 0.33b provides in part that the Counsel for Intelligence policy shall:

> (e) Evaluate Departmental activities and existing and proposed domestic and foreign intelligence and counterintelligence activities to determine their consistency with United States intelligence policies and law; . . . and (g) Analyze and interpret current statutes, Executive orders, guidelines, and other directives pertaining to domestic security, foreign intelligence and counterintelligence activities . . ." (Emphasis added.)

Accordingly, we believe the FBI and DOJ should confer about the FBI's current interpretation of this Guidelines' requirement, particularly in view of the implications for review of terrorism-related investigations arising from the establishment of a National Security Division within the Department of Justice and FBI's new National Security Service. The results of these consultations should be reported to the OIG.

22. **Resolved.** In response to this recommendation that the FBI discuss with DOJ how to reconcile Section 100-2.3(3) of the MIOG, requiring Headquarters' concurrence with the initiation and renewal of terrorism enterprise investigations, with Sections III.B.4a & b of the General Crimes Guidelines, which authorize field level initiation and renewal of these investigations, the FBI stated that it concurs with the recommendation. The FBI stated that it requires FBI Headquarters' concurrence of SAC authorization "to ensure centralized program management of these investigations, which typically involve groups with a nation-wide presence, and to permit higher level review of these sensitive investigations that usually implicate first amendment concerns." The FBI stated that it will discuss the matter with DOJ to pursue an appropriate reconciliation.

Accordingly, please provide details of the resolution resulting from the consultation between the FBI and DOJ representatives, together with any guidance or notifications regarding the resolved interpretation.

23. **Resolved.** In response to this recommendation that the FBI require field-level supervisory approval, absent exigent circumstances, prior to the exercise of Part VI.A.2 authorities to visit public places or attend public events for the purpose of detecting or preventing terrorism, the FBI stated that it concurs with this recommendation.

Accordingly, please provide the standardized form, guidance, and notifications that the Counterterrorism Division distributes to implement this recommendation.

24. **Unresolved.** In response to this recommendation that the FBI develop a standardized form or short e-mail template to be completed by case agents documenting their use of Part VI.A.2 authorities in the General Crimes Guidelines, the FBI stated that it concurs with this recommendation. However, the FBI stated only that the Counterterrorism Division will request that this statistic be captured as part of the re-engineering process.

While we believe it is important for the FBI to capture statistics on its use of Part VI.A.2 authorities to visit public places or attend public events for the purpose of detecting or preventing terrorism, we believe that FBI agents should use a standardized form or template to document their use of these authorities (e.g., date of visit, group or event monitored, and short justification for the monitoring), not merely to capture statistics. Accordingly, we do not believe the FBI's response adequately addressed the intent of this recommendation. We ask the FBI to reconsider developing a standardized form to be completed by case agents documenting their use of Part VI.A.2 authorities in the General Crimes Guidelines, together with guidance and notifications necessary to implement this recommendation.

25. **Resolved.** In response to this recommendation that the FBI consider whether field offices practices since May 30, 2002, regarding predication, collection, record retention, indexing, and dissemination of Part VI.A information, and practices regarding utilization of "zero files" or other files used to capture Part VI.A information, are in conformity with the Guidelines and FBI guidance; whether there is need for further guidance on these subjects; and whether FBI Headquarters managers should have access to data reflecting use of Part VI.A.2 authorities, the FBI stated that it concurs with the recommendation. The FBI stated that the Counterterrorism Division will consult with the Office of the General Counsel to review existing guidance and to determine whether additional guidance is needed.

Accordingly, please provide the results of the FBI's review of existing guidance and any new guidance, together with the notifications necessary to implement this recommendation.

26. **Resolved.** In response to this recommendation that the FBI ensure that required authorizations for consensual monitoring are obtained in advance and are appropriately documented, the FBI stated that it concurs with the recommendation.

Accordingly, please provide details regarding how the FBI intends to ensure that required authorizations for consensual monitoring are obtained in advance and are appropriately documented.

27. **Resolved.** In response to this recommendation that the FBI consult with DOJ to resolve whether, for purposes of monitorings that do not require DOJ approval, the Consensual Monitoring Guidelines should be interpreted to authorize monitoring for more than 90 days (including up to "the duration of the investigation" as currently provided on Form FD-759), or whether the authorization is limited to 90 days, and to incorporate any clarification of policy in the FBI's MIOG, the FBI stated that it concurs with the recommendation. According to the FBI, by letter dated August 25, 2005, the Director of the DOJ Criminal Division's Office of Enforcement Operations (OEO), advised that the Consensual Monitoring Guidelines should be interpreted to authorize monitoring for more than 90 days (including up to "the duration of the investigation" as currently provided on Form FD-759).

Accordingly, please provide a copy of OEO's letter and any resulting guidance and notifications necessary to implement this recommendation.

28. **Resolved.** In response to this recommendation that the FBI provide CUORC members, upon request, with access to copies of Inspection reports concerning undercover operations, the on-site reviews conducted by the Undercover and Sensitive Operations Unit, and after-action reports of undercover operations, the FBI stated that it concurs with the recommendation. The FBI further stated that the Unit Chief of the Undercover and Sensitive Operations Unit has coordinated this recommendation with an Assistant Inspector of the Inspection Division.

However, the FBI did not specifically address the portion of our recommendation that CUORC members, upon request, also be provided copies of the Undercover and Sensitive Operations Unit's on-site reviews and after-action reports of undercover operations.

Accordingly, please provide provides details of the procedures and notifications the FBI has made in implementing this recommendation with respect to the availability of Inspection reports to CUORC members and the availability to CUORC members of on-site reviews and after-action reports.

29. **Resolved.** In response to this recommendation that the FBI consider ways for the Undercover and Sensitive Operations Unit to develop more complete information for the CUORC and other FBI components, including information such as trend analysis from on-site reports, persistent Guidelines violations, and copies of its semi-annual report to all FBI Headquarters operating divisions, the FBI stated that it concurs with the recommendation.

Accordingly, please provide details as to how the Undercover and Sensitive Operations Unit develops more complete information for the

CUORC and other FBI components, particularly with regard to trend analysis of on-site reports and persistent Guidelines violations.

30. **Resolved.** In response to this recommendation that the FBI require that the initial and continuing suitability reviews of confidential informants contain more thorough answers to suitability questions to assist CIRC members in evaluating confidential informants and assist field and Headquarters managers in their supervisory responsibilities, the FBI stated that it concurs with the recommendation.

Accordingly, please provide copies of the revised initial and continuing suitability forms, together with any guidance and notifications necessary to implement this recommendation.

31. **Resolved.** In response to this recommendation that the FBI consider having the Human Intelligence Unit draft "lessons learned" from the CIRC's decisions, periodically communicate these lessons to field personnel, and incorporate them into training on the Confidential Informant Guidelines, the FBI stated that it concurs with the recommendation.

Accordingly, please provide materials regarding "lessons learned" from the CIRC's decisions, together with any guidance and notifications necessary to implement this recommendation.

32. **Resolved.** In response to this recommendation that the FBI make available to CIRC members, upon request, copies of the Inspection Division's audits of the Criminal Informant Program (including re-inspection reports) and evaluations performed by the Human Intelligence Unit of compliance with the Confidential Informant Guidelines, the FBI stated that it concurs with the recommendation. However, the FBI stated that it will "consider" requests from the CIRC for these reports and materials and does not believe it is necessary for the DOJ representatives on the CIRC to receive this information in order to carry out the CIRC's essential purposes.

We believe the Inspection Division's audits of the Criminal Informant Program (including any reinspection reports) and the Guidelines-related evaluations performed by the Human Intelligence Unit can provide highly useful information for all members of the CIRC. Accordingly, we believe that the FBI should provide this information to CIRC members, upon request. Please provide any FBI guidance and notifications implementing the FBI's response to this recommendation.

33. **Resolved.** In response to this recommendation that the FBI revise the Inspection Division's checklists and interrogatories to increase inspection coverage of Guidelines-related issues, the FBI stated that it concurs with the recommendation.

Accordingly, please provide copies of the revised checklists and interrogatories, together with any guidance and notifications necessary to implement this recommendation.

34. **Resolved.** In response to this recommendation that the FBI establish an audit examining the collection of information obtained from the exercise of counterterrorism authorities pursuant to Part VI.A.2 (Visiting Public Places and Events) of the General Crimes Guidelines, the FBI stated that it concurs with the recommendation.

However, when the OIG reviewed the July 2005 checklist, we determined that it does not provide adequate direction for collecting data regarding the FBI's use of Part VI.A.2 authorities. We provided suggestions for a revised checklist that would capture this data. Accordingly, please provide information regarding the new audit, and the revised checklist, together with any guidance and notifications necessary to implement this recommendation.

35. **Resolved.** In response to this recommendation that the FBI provide more thorough and timely reporting of Guidelines violations by identifying in inspection reports the causes and gravity of compliance deficiencies; developing summary statistics to assist in determining when re-inspections are appropriate; and automating key components of the inspection process, the FBI stated that it concurs with the recommendation. The FBI further stated that the Inspection Division's Criminal Informant Program checklists have been revised to collect information of the causes of identified deficiencies and that the Inspection Division is in the process of creating a computer database to assist in analyzing the results of compliance audits.

Accordingly, please provide copies of the revised checklists and a description of the new automation and other procedures to be employed in analyzing the results of compliance audits, together with any guidance and notifications necessary to implement this recommendation.

36. **Resolved.** In response to this recommendation that the FBI increase inspections for the Criminal Informant Program and other program priorities by performing more frequent inspections at irregular times, develop a standard for re-inspections that accounts for the frequency and seriousness of Guidelines deficiencies identified during the regular inspection, and reinstate the reinspection process initiated by the Human Intelligence Unit (formerly the Asset/Informant Unit), the FBI stated that it concurs with the recommendation.

Accordingly, please provide details of the FBI's revised inspections plan, its standard for re-inspections, and instructions regarding the

reinstitution of the Human Intelligent Unit's reinspection process, together with any guidance and notifications necessary to implement this recommendation.

37. **Resolved.** In response to this recommendation that the FBI address in employee performance appraisals the findings from Inspection Division inspections that identify either superior or deficient Guidelines compliance performance, the FBI stated that it concurs with the recommendation and will explore ways to accomplish this goal within the limits of the regulations that govern this process as well as the limitations of the FBI Performance Appraisal System.

Accordingly, please provide details of the review of the FBI's employee performance appraisals and any revisions that address pertinent Guidelines compliance findings from Inspection Division reports, together with any guidance and notifications necessary to implement this recommendation.

38. **Resolved.** In response to this recommendation that the FBI elevate egregious non-compliance with the Attorney General Guidelines to an executive management finding in inspection reports rather than deferring that action until the next 3-year inspection, contingent on the detection of recurring, serious deficiencies, the FBI stated that it concurs with the recommendation.

Accordingly, please provide copies of any guidance and notifications necessary to implement this recommendation.

39. **Resolved.** In response to this recommendation that the Inspection Division and the Human Intelligence Unit in the Directorate of Intelligence institute procedures that establish follow-up inspection measures to re-inspections that indicate on-going compliance problems, the FBI stated that it concurs with the recommendation.

Accordingly, please provide details of the new follow-up inspection procedures, together with any guidance and notifications necessary to implement this recommendation.

40. **Resolved.** In response to this recommendation that the FBI modify the Undercover and Sensitive Operations Unit's on-site review data collection instrument to better address Guidelines compliance (including issues such as otherwise illegal activity, entrapment, and task force participation), the FBI stated that it concurs with the recommendation.

Accordingly, please provide copies of the revised data collection instrument, together with any guidance and notifications necessary to implement this recommendation.

41. **Resolved.** In response to this recommendation that the FBI ensure that Attorney General Guidelines' violations warranting potential discipline are referred to the FBI's Internal Investigations Section in the Inspection Division in a consistent fashion throughout the FBI, the FBI stated that it concurs with the recommendation.

Accordingly, please provide copies of any guidance and notifications necessary to implement this recommendation.

42. **Resolved.** In response to this recommendation that the FBI ensure that the Inspection Division's standards for referring misconduct involving Guidelines violations are consistent with practices adopted by the Inspection Division's Internal Investigations Section, the FBI stated that it concurs with the recommendation. The FBI further stated that a new process has already been implemented by the Inspection Division.

Accordingly, please provide a description of the new processes in place in response to this recommendation, together with any guidance and notifications necessary to implement this recommendation.

43. **Resolved.** In response to this recommendation that the FBI add separate offense codes for (i) knowingly or recklessly failing to obtain proper authorization for a source's participation in otherwise illegal activity; (ii) knowingly or recklessly failing to obtain proper authorization to operate long term, high-level, privileged or media-affiliated confidential informants or other informants subject to special approval requirements; and (iii) knowingly or recklessly failing to operate long-term, high-level, privileged or media-affiliated confidential informants, or other informants subject to special approval requirements in accordance with the relevant Confidential Informant Guidelines and MIOG provisions, the FBI stated that it concurs with the recommendation. The FBI stated that a team from the Inspection Division and the Office of Professional Responsibility has been formed to ensure that the three new offense codes are added in accordance with the relevant Confidential Informant Guidelines and MIOG provisions.

Accordingly, please provide us with the revised offense codes and any related guidance necessary to implement this recommendation.

44. **Resolved.** In response to this recommendation that the FBI assign some person or unit at FBI Headquarters the responsibility to develop a plan to ensure proper and timely execution of future Attorney General Guidelines revisions and to coordinate implementation of the revisions over time, the FBI stated that it concurs with the recommendation. The FBI further stated that it will determine the best way to implement the recommendation.

Accordingly, please provide a description of the new procedures, together with any guidance and notifications necessary to implement this recommendation.

45. **Resolved.** In response to this recommendation that the FBI distribute revised Attorney General Guidelines to Chief Division Counsel, together with a concise summary or listing of the changes, sufficiently in advance of the new Guidelines' effective date to allow field personnel to familiarize themselves with the revisions and to allow those Headquarters and field personnel who provide training on the revisions to develop training materials and a schedule for providing training, the FBI stated that it concurs with the recommendation.

Accordingly, please provide a description of the new procedures, together with any guidance and notifications necessary to implement this recommendation.

46. **Resolved.** In response to this recommendation that the FBI ensure that revisions to the MIOG accurately reflect any changes to the Attorney General's Guidelines and are made on or about the effective date of such changes, the FBI stated that it concurs with the recommendation. The FBI notes, however, that "if a considered agency decision is made to impose more restrictive procedural requirements in the MIOG for agency oversight purposes than those required by the Guidelines, then such distinctions and the reasons therefore be documented and explained in the MIOG revisions."

As stated in our report, the MIOG is the FBI's official reference guide on operational procedures. It is vital that it be fully updated when the Guidelines changes or soon thereafter. However, we found that requests for changes to the MIOG were received by the FBI's Records Management Division from 2 to 11 months after the May 2002 Guidelines changes were issued. We also found that some updates to the MIOG were not completed until more than two years after the revised Guidelines became effective.

In addition, we note that, using the FBI's current technology, revision of the MIOG involves several steps, including requests for revisions from the substantive unit, logging of the revision into the FBI's mainframe automated manuals application, followed by uploading into SOFTBOOK and, ultimately, the FBI's Intranet.

Accordingly, please provide details of how the FBI plans to ensure that revisions to the MIOG accurately reflect any changes to the Attorney General's Guidelines and are made on or about the effective date of such changes together with any guidance and notifications necessary to implement this recommendation.

47. **Resolved.** In response to this recommendation that the FBI make appropriate changes to the MIOG to reconcile the discrepancies between the Attorney General's Guidelines and the MIOG that are identified in the report, the FBI stated that it concurs with the recommendation "when true discrepancies exist."

Accordingly, please provide details on its resolution of the discrepancies identified in the report and any revised MIOG provisions, together with any guidance and notifications necessary to implement this recommendation.

# APPENDIX I

# LIST OF ACRONYMS

| | |
|---|---|
| ABSCAM | FBI sting operation |
| ACS | Automated Case System |
| AD | Assistant Director (FBI) |
| ADIC | Assistant Director in Charge |
| AAG | Assistant Attorney General |
| AGG | Attorney General Guidelines |
| A/IU | Asset/Informant Unit |
| ASAC | Assistant Special Agent in Charge |
| ATF | Bureau of Alcohol, Tobacco, Firearm and Explosives |
| CDC | Chief Division Counsel |
| CFR | Code of Federal Regulations |
| CI | Confidential Informant |
| CIC | Confidential Informant Coordinator |
| CID | Criminal Investigative Division |
| CIO | Chief Information Officer |
| CIP | Criminal Informant Program |
| CIRC | Confidential Informant Review Committee |
| CISPES | Committee in Solidarity with the People of El Salvador |
| CM | Consensual Monitoring |
| CUORC | Confidential Undercover Operation Review Committee |
| CS | Confidential Source |
| CSR&R | Continuing Suitability Report and Recommendations |
| CTD | Counterterrorism Division |
| CW | Cooperating Witness |
| DEA | Drug Enforcement Administration |
| DI | Directorate of Intelligence |
| DIA | Delegated Investigation/Adjudication |
| DIO | Delegated Investigation Only |
| DOJ | Department of Justice |
| DRB | Disciplinary Review Board |
| EC | Electronic Communication |
| ELSUR | Electronic Surveillance |
| FAQ | Frequently Asked Question |
| FBI | Federal Bureau of Investigation |

| | |
|---|---|
| FBIHQ | Federal Bureau of Investigation Headquarters |
| FCI | Foreign Counterintelligence Investigation |
| FGUSO | Field Guide for Undercover and Sensitive Operations |
| FIG | Field Intelligence Group |
| FOIA | Freedom of Information Act |
| GAO | General Accountability (formerly Accounting) Office |
| GCI | General Crimes Investigation |
| GPO | Government Printing Office |
| GS | General Schedule |
| HIU | Human Intelligence Unit |
| IB | Intelligence Base |
| IIS | Internal Investigations Section (FBI) |
| IIU | Internal Investigative Unit |
| ILU | Investigative Law Unit |
| INS | Immigration and Naturalization Service |
| IPU | Initial Processing Unit |
| ISR&R | Initial Suitability Report and Recommendations |
| JLEA | Department of Justice Law Enforcement Agency |
| LCN | La Cosa Nostra |
| LEEU | Law Enforcement Ethics Unit |
| LEGAT | Legal Attaché |
| LMRDA | Labor-Management Reporting and Disclosure Act |
| MAOP | Manual of Administrative Operations and Procedures |
| MIOG | Manual of Investigative Operations and Guidelines |
| NCIC | National Crime Information Center |
| NSI | National Security Investigation |
| NTCM | Nontelephonic Consensual Monitoring |
| OCRS | Organized Crime and Racketeering Section |
| OGC | Office of the General Counsel |
| OIA | Otherwise Illegal Activity |
| OIG | Office of the Inspector General |
| OIPR | Office of Intelligence Policy and Review |
| OPEA | Office of Program Evaluations and Audits |
| OPEAU | Organizational Program, Evaluation and Analysis Unit |
| OPR | Office of Professional Responsibility |

| | |
|---|---|
| PI | Preliminary Inquiry |
| REI | Racketeering Enterprise Investigation |
| RICO | Racketeer Influenced and Corrupt Organizations Act |
| RMD | Records Management Division |
| SAC | Special Agent in Charge |
| SCLC | Southern Christian Leadership Conference |
| SES | Senior Executive Service |
| SID | State Identification Number |
| SIS | Suitability Inquiry Status |
| SR&R | Suitability Report and Recommendations |
| SSA | Supervisory Special Agent |
| SWP | Socialist Workers Party |
| TEI | Terrorism Enterprise Investigation |
| UCC | Undercover Coordinator |
| UCO | Undercover Operation |
| UIA | Unauthorized Illegal Activity |
| UORC | Undercover Operation Review Committee |
| USAO | United States Attorney's Office |
| USOU | Undercover and Sensitive Operations Unit |
| VCF | Virtual Case File |