

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 1

SECTION 10. RECORDS AVAILABLE AND INVESTIGATIVE TECHNIQUES

10-1 INTRODUCTION

(1) The following information is being provided as a reference for investigative personnel seeking additional data and/or the location of individuals who are the subjects of FBI investigations. This information is presented in two parts, Records Available and Investigative Techniques.

(a) Records Available are those documents which may assist in either compiling a necessary profile (either of a group, an individual or a business enterprise), or will assist in locating subjects, suspects, witnesses or victims.

(b) An Investigative Technique is a method by which an activity is conducted (Title III) or information placed (stop notice) which may aid in the identification or location of a subject or in the gathering of evidence.

(2) The use of any of these records or investigative techniques must be in accord with legal and ethical investigative procedures. In many cases, the obtaining of records or use of an investigative technique must be authorized by the SAC, Department of Justice, Attorney General or court order. If any doubt exists as to what the correct procedure is, the appropriate supervisory personnel must be consulted. It should be additionally noted that the information contained in this section is not all-inclusive regarding records or investigative techniques available.

(3) As the various items appear, there will be either a reference to another section in this manual or to another manual, an explanation of what the technique is or simply a listing of the record. Additional record information is available in Part II, Section 19 of this manual titled, "Location of Other Government, Industrial, and Organizational Records."

EFFECTIVE: 01/21/86

Sensitive  
PRINTED: 02/18/98

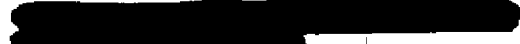
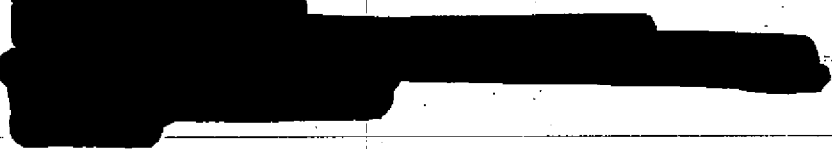
Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 2

10-2 RECORDS AVAILABLE


  
Biographic Directories

  
  
City Directory  
Closed and Pending Files  
Court System

|| Department of Veterans Affairs |  


Field Office Special Services List  


b2, b7E

Government Agencies  


Identification Records (FD-9)  


Interstate Identification Index  


Maps

Marriage Records

Merchant Marine

Military Departments

Motor Vehicle Department  


National Auto Theft Bureau

Newspaper Library  


PD Checks  


Probation and Parole Offices

Public Libraries  


Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 3

Schools and Colleges  
Social Security Records  
Sources of Information Index  
Street Guide  
Surveillances

Telephone Directory

Unemployment Agencies, Federal and State

b2, b7E

Voter Records

EFFECTIVE: 05/25/90

10-3 INVESTIGATIVE TECHNIQUES (See MIOG, Part II, 21-23  
(25).)

Artist Conceptions	see MIOG, Part II, 13-24
Crime Scene Searches	see MIOG, Part II, 13-6.4
Check Circulars	see MIOG, Part II, 21-25
Circular Letters	see MIOG, Part II, 21-24
Computer Assistance or Automatic Data Processing	see MIOG, Part II, 10-4
Interstate Identification Index (III)	see MIOG, Part II, 10-5
Consensual Monitoring	see MIOG, Part II, 10-10
Electronic Surveillance (ELSUR)	see MIOG, Part II, 10-9
Evidence -	
Racketeering Records Analysis	see MIOG, Part II, 13-20
Collection, Identification and Preservation of Physical Evidence	see MIOG, Part II, 13-6.4.7

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 4

Collection of Evidence in Rape Cases see MIOG, Part II, 13-8.2.5

Fluorescent Powders and Other Marking Materials see MIOG, Part II, 13-15.2

Plastic Cast Impression of Stamped Numbers in Metal see MIOG, Part II, 13-13.3.1

Restoration of Obliterated Markings see MIOG, Part II, 13-14.2

(10)

Shoe/Tire Tread Cast and Lifts see MIOG, Part II, 13-19

Hypnosis see MIOG, Part II, 10-12

Identification Orders see MIOG, Part II, 21-25

Informants see MIOG, Part I, 137

Investigative Information Services Data Bases For Use In Investigations see MIOG, Part II, 10-17

Mail Covers see MIOG, Part II, 10-6

National Crime Information Center see MAOP, Part II, 7

Pen Registers see MIOG, Part II, 10-10.7

Photographic Examinations see MIOG, Part II, 13-7.6

Photographic Surveillances see MIOG, Part II, 13-7.5

Polygraph Examinations see MIOG, Part II, 13-22

Stop Notices see MIOG, Part II, 10-7

Surveillance Techniques see MIOG, Part II, 9

Telephone Toll Records see MIOG, Part II, 10-8

Title III Coverage see MIOG, Part II, 10-9.10

Undercover Activities

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 5

Criminal Matters	see MIOG, Part II, 10-11
Wanted Flyers	see MIOG, Part II, 21-25
Wanted or Flash Notices on Fingerprint Cards	see MIOG, Part II, 14-15.5

EFFECTIVE: 07/25/97

10-4 COMPUTER ASSISTANCE OR AUTOMATIC DATA PROCESSING (See  
MIOG, Part II, 10-3.)

The Investigative Automation Support Section of the Information Resources Division assists the field in investigative matters: (1) involving computer or data processing personnel; (2) where there are voluminous records that require sequencing, comparison or calculations; (3) requiring assistance in the wording of subpoenas for computer records; or search warrants for searching of computer installations, etc. More detailed information regarding computer services available to you is set forth in Part II, 16-10, of this manual.

EFFECTIVE: 06/01/94

10-5 INTERSTATE IDENTIFICATION INDEX (III) (See MIOG, Part II,  
10-3; MAOP, Part II, 7-4.1.)

(1) The III allows on-line accessibility of criminal arrest records through the use of your NCIC computer terminal. The III maintains index records which contain personal descriptive data of the subject of the criminal history record. The location of the data base(s) which stores the criminal history record is also part of the Index. Records available through the III include: subjects arrested with dates of birth 1956 or later and all individuals arrested for the first time on or after 7/1/74, regardless of their dates of birth and selected older records converted to the automated system for certain fugitives and repeat offenders.

(2) Detailed instructions for conducting name searches

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 6

and record retrievals are set forth in Part 10 of the NCIC OPERATING MANUAL. The state control terminal officer within your state can respond to any questions or problems you might have concerning the operation of your NCIC computer terminal.

(3) All field offices are encouraged to use III in their daily operations.

(4) If no record is located through the III File, check with the FBI Criminal Justice Information Services Division since it maintains over 10 million additional records not available through III.

EFFECTIVE: 05/13/96

10-6 MAIL COVERS

EFFECTIVE: 03/09/81

10-6.1 United States Postal Service (USPS) Regulations

(1) USPS regulations governing mail covers are codified in Title 39, Code of Federal Regulations (CFR), Section 233.2 and designate the Chief Postal Inspector to administer all matters governing mail cover requests by law enforcement agencies. Except for national security mail covers, the Chief Postal Inspector may delegate any or all such authority to the Regional Chief Postal Inspectors. In addition, all Postal Inspectors in Charge and their designees are authorized to order mail covers within their districts in fugitive and criminal matters.

(2) USPS regulations state that a mail cover may be requested to locate a fugitive, to obtain information regarding the commission or attempted commission of a crime, or to protect the national security.

(3) For mail cover purposes, a "mail cover" is defined by USPS as the process by which a record is made of any data appearing on the outside cover of any class of mail matter, (the FBI may not request a check of the contents of any class of mail); a "crime" is defined as the commission or attempted commission of an act punishable

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 7

by imprisonment for a term exceeding one year; a "fugitive" is any person who has fled from the United States or any state, territory, the District of Columbia, or possession of the United States, to avoid prosecution for a crime or to avoid giving testimony in a criminal proceeding.

(4) No mail covers shall include matter mailed between the mail cover subject and subject's known attorney-at-law. However, the mere fact that a subject has retained an attorney will not defeat a mail cover. A mail cover may be used but mail between the subject and subject's attorney shall not be included. Mailed matters between the subject and subject's attorney are protected.

(5) Excepting fugitive cases, no mail cover shall remain in force when the subject has been indicted for any cause. If the subject is under investigation for further criminal violations, a new mail cover order must be requested consistent with USPS regulations. A mail cover on an indicted subject who is not a fugitive is still possible under certain conditions. Although not available for crimes for which the subject has been indicted, a mail cover may be used as an investigative tool to investigate the subject's other crimes. As to fugitives, a mail cover is available for the offense for which indicted and other crimes.

(6) Excepting mail covers ordered upon subjects engaged, or suspected to be engaged, in any activity against the national security, or activity violative of any postal law, no mail cover order shall remain in force for more than 30 days. At the expiration of such period or prior thereto, the requesting authority may be granted additional 30-day periods under the same conditions and procedures applicable to the original request. No mail cover shall remain in force longer than 120 days unless personally approved for further extension by the Chief Postal Inspector. In all requests for mail covers to extend beyond 120 days, the requesting authority must specify the reasonable grounds that exist which demonstrate the mail cover is necessary for one of the stated purposes.

(7) No officer or employee of the USPS other than the Chief Postal Inspector, Postal Inspectors in Charge or their designees are authorized to order mail covers. Under no circumstances shall a postmaster or postal employee furnish information, as defined in paragraph (3), to any person except as authorized by the Chief Postal Inspector, Postal Inspector in Charge or their designees.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 8

EFFECTIVE: 03/09/81

10-6.2 Policy

(1) SAC approval must be obtained before a mail cover request is submitted to the USPS. SACs are authorized to request mail covers, with the exception of those involving National Security cases, from the USPS. See policy in Part II, 10-6.3.2 concerning mail covers involving National Security cases.

(2) In criminal matters, requests for mail covers should be submitted when it can be shown that use of the technique would be logical, resourceful, appropriate, and when the use of the technique is in conformance with all regulatory requirements and guidelines including the Attorney General's Guidelines on General Crimes, Racketeering Enterprises, and Domestic Security/Terrorism Investigations. When requesting authorization to utilize a mail cover, consideration should be given to whether the information sought can be obtained in a timely and effective manner by less intrusive means. Further, in recognition that use of a mail cover raises possible First Amendment concerns, care should be taken to ensure use of the mail cover will be confined to the immediate needs of the investigation, particularly when considering a mail cover to be placed on an individual who is not the subject of a criminal investigation.

(3) The SAC should review and approve all requests for mail covers and should review and approve all requests for continuation of existing mail covers.

(4) The SAC should conduct frequent checks as to the productivity of mail covers after being placed into effect.

(5) Cases are not to be closed until the mail cover has expired or has been withdrawn. SAC must be notified if request for mail cover is not approved by the USPS, which notification shall include a statement of the reasons given by the postal authorities for not approving the mail cover request.

(6) Information obtained as a result of a mail cover in fugitive or criminal cases should be reported in the cover pages.

(7) Requests for mail covers should not be submitted in preliminary criminal inquiry investigations. ("The Attorney General's Guidelines on General Crimes, Racketeering Enterprises, and Domestic

Sensitive

PRINTED: 02/18/98



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 9

Security/Terrorism Investigations," effective 3/21/83.)

(8) A mail cover index is to be maintained by the Administrative Officer/Office Services Manager. 3- by 5-inch cards, FD-57, may be filed alphabetically or by street address and should reflect the following:

- (a) Name and address of person whose mail is covered
- (b) Fugitive or criminal case
- (c) File number of case
- (d) Date when placed
- (e) Identity of Agent handling
- (f) City
- (g) Duration of mail cover

(9) After the mail cover has been discontinued, the mail cover index card is to be destroyed.

EFFECTIVE: 05/09/95

10-6.3 Requesting Approval

EFFECTIVE: 05/09/95

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 10

10-6.3.1 Fugitive or Criminal Cases

(1) In recommending a mail cover in a FUGITIVE OR CRIMINAL CASE, submit a memo to the SAC advising that a mail cover is being requested from the district Postal Inspector in Charge covering the area where the mail cover is to be placed.

(2) This memo must also include the following information:

(a) Brief background of the case.

(b) A statement setting forth the reasons that the use of a mail cover is logical, resourceful and appropriate.

(c) Identity and complete mailing address of the person whose mail is to be covered.

(d) Location of the district Postal Inspector in Charge to be utilized.

(e) The federal statute and maximum possible penalty involved.

(f) Whether the person whose mail is to be covered is under indictment in connection with the matter under investigation.

(g) Whether the person whose mail is to be covered is known to have retained an attorney and, if so, the attorney's name.

(h) In fugitive cases, whether the fugitive is under indictment in connection with the matter under investigation.

(i) In fugitive cases, whether the fugitive is known to have obtained an attorney and, if so, the attorney's name.

(3) Your request to the appropriate district Postal Inspector in Charge must be written or confirmed in writing.

(4) In fugitive and criminal cases, mail covers may be placed initially for 30 days' duration and may be extended on request to the district Postal Inspector in Charge for additional 30-day periods up to a total of 120 days. If an extension of the mail cover beyond this 120-day period is desired, submit the request for an extension to the appropriate USPS authority. Any request for extension beyond 120 days must clearly set forth any specific

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 11

reasonable grounds that exist which demonstrate the mail cover is NECESSARY.

(5) SAC approval is required when requesting that confidential arrangements be made to initiate a particular mail cover. The period of days of the mail cover must be specified, but a particular date should not be.

(6) When emergency authority is needed to establish a mail cover, USPS regulations state that the appropriate Postal Inspector in Charge, or that Inspector's designee may act upon an oral request, to be confirmed by the requesting authority in writing within two business days. However, the USPS will release no information until an appropriate written order is received.

EFFECTIVE: 05/09/95

10-6.3.2 National Security Cases

(1) As noted above, USPS regulations state that a mail cover may be requested to protect the national security. For mail cover purposes, "to protect the national security," is defined by USPS as protecting the United States from any of the following actual or potential threats to its security by a foreign power or its agents: (i) an attack or other grave hostile act; (ii) sabotage, or international terrorism; or, (iii) clandestine intelligence activities.

(2) All mail covers in national security cases must be approved personally by the Director of the FBI or, in Director's absence, by the Acting Director on Director's behalf. If the individual on whom the mail cover is to be placed is a United States person, Attorney General approval is also required.

(3) All correspondence concerning national security mail covers should be transmitted "BY LIAISON" and addressed as follows:

Chief Postal Inspector  
U.S. Postal Service  
475 L'Enfant Plaza, Southwest  
Washington, D.C. 20260  
Attention: Legal Liaison Branch

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 12

Room 3417

(4) The name and address of the individual or establishment on which the mail cover is to be placed must be unclassified. A statement such as "For the purpose of placing the mail cover, the above-captioned individual's name and address are considered unclassified," will suffice.

(5) In these national security cases, when the field is recommending to FBIHQ that a mail cover be requested, complete information concerning the name and address of each individual or organization to be covered, including ZIP code, should be supplied. Set forth information similar to that outlined above for criminal cases, including any information concerning known attorneys of record and any information as to whether or not the subject is under indictment. Requests for approval of national security mail covers will require more detailed explanations and must stipulate and specify the reasonable grounds that exist which demonstrate the mail cover is necessary to protect the United States from an actual or potential threat to its national security.

(6) If the request for a mail cover in a national security case is approved by FBIHQ, arrangements for implementing the mail cover will be handled by FBIHQ.

EFFECTIVE: 02/16/89

10-7 STOP NOTICES

EFFECTIVE: 06/10/88

10-7.1 Definition

A stop notice is a request to be advised if an individual or property comes to the attention of any organization or a member thereof.

EFFECTIVE: 06/10/88

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 13

10-7.2 Placement of Stops

The form utilized for placement of stops is an FD-56, a 3- by 5-inch card. This should record the date a request is made of a particular law enforcement agency, [REDACTED] etc. This form should not be prepared if information has previously been furnished NCIC unless a reason exists otherwise. If so, it should be indicated on FD-56. The office placing the stop should prepare the FD-56 and route to the office of origin (OO) by letter or as an enclosure to another communication setting forth the results of investigation. This communication should include the name of the Agent placing the stop and with whom the stop was placed.

b2, b7E

EFFECTIVE: 06/10/88

10-7.3 Indexing Stops

(1) The requesting and placing offices are required to record in their automated indices each name and/or item of property which is documented in a stop notice while the stop notice is in force (subject or reference record). The miscellaneous part of the index record should contain the same information as included on the FD-56.

(2) The Office of Origin (OO) will file the FD-56 in the manual general index except when FBIHQ is OO. If FBIHQ is OO, the office placing the stop will maintain the FD-56 in its manual general index. The FD-56 will be filed with the manual general index before the letter group "A" led by a separator marked "STOP NOTICES" and sequenced in proper numerical order (Classification, Case, Serial). If the stops were placed by a written communication, only one card is needed even though more than one item was listed. When stops have been placed with FBIHQ or by another field office, no cards (FD-56s) are necessary.

EFFECTIVE: 06/10/88

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 14

10-7.4 Removal of Stops

(1) It is the direct responsibility of the OO to remove all stops on individuals or property when a determination has been made that they are no longer needed. Stop cards are to be reviewed quarterly to remove obsolete cards and to discontinue unnecessary stops.

(2) Mechanics of removing stops - Office of origin will forward, via routing slip, FD-56 to office which placed stop advising stop should be removed. Notation will be made on appropriate serial in file indicating name of employee and date stop removed after which FD-56 will be destroyed. Office of origin should be advised of removal of a stop by the office which placed the stop.

EFFECTIVE: 06/10/88

10-7.5 Types of Stops

EFFECTIVE: 06/10/88

10-7.5.1 [REDACTED]

Stop notices are placed by letter to [REDACTED]

b2, b7E

EFFECTIVE: 06/10/88

10-7.5.2 Immigration and Naturalization Service (INS)

These stops (INS Lookout Notices) are placed by use of the FD-315 form. The original FD-315 must be signed by the approving field supervisor and sent directly to INS as indicated on the form. INS will not place stops on U.S. citizens since it has no statutory authority over U.S. citizens.

(1) INS stops are of necessity never classified. The stop names and identifiers are available on lists or electronically in

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE - 10 - 15

areas open to travelers.

(2) INS regulations state that other Federal agencies may request the posting of lookouts. These requests for stops must meet the INS criteria for posting unless there are outstanding warrants of arrest, [REDACTED]

[REDACTED] FBI investigative activity does not usually meet INS criteria for posting lookouts.

b7E per INS

(3) The INS Stop System consists of three parts: (a) The INS "National Automated Immigration Lookout System" (NAIIS), an automated telecommunications network records system; (b) The "INS Lookout Book" printed with one-line lookout records, updated and distributed once every calendar month; and (c) A 90-day temporary emergency lookout system posted electronically by INS Central Office, or by local FBI Border Offices.

(4) [REDACTED] INS stops will be posted until the subject's ninetieth birthday.

b7E per INS

(5) Instructions for Completing FD-315 - Instructions are printed on the reverse of the FD-315 form. One subject should appear on a single form with additional names or aliases listed alphabetically on that form. Do not use spelling variations. Only actual names used by subject or those names for which subject is known to have identification should be submitted. One birthday only should be used. If the subject is considered armed and dangerous, suicidal or having physical or mental problems, the caution block should be checked (x'd) and this information should be explained under "Miscellaneous."

The FD-315 lists [REDACTED]

(a) [REDACTED]

(b) [REDACTED]

(c) [REDACTED]

b7E per INS

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 16

(6) Emergency INS Border Stops - A teletype can be forwarded to INS Headquarters requesting an emergency INS stop. In addition, border FBI offices may place stops with INS at a local level along the Canadian and the Mexican borders. In order to handle such stops these offices must be provided with: identity; description; photograph, if available; approximate time subject expected and mode of travel. Emergency stops should be placed selectively when all of the above items are not available. In addition, when it becomes apparent these stops will extend beyond 90 days, an FD-315 should be sent to INS, Washington, D.C.

(7) ~~Cancellation and Amending of INS Stops~~ - It is incumbent upon the requesting office to place and cancel stops. The FD-315 should also be used to amend or provide additional pertinent information developed on subject. In all cases the FD-315 should be used and the proper action is to be indicated. Stops are cancelled automatically by INS at the end of the period indicated. Note: the maximum time an INS stop can be in effect by submission of an FD-315 is five (5) years. If no cancellation date is shown on the FD-315, INS will place the stop for a maximum of one (1) year. The requesting office should be on the alert to renew these stops if required.

EFFECTIVE: 05/25/90

[REDACTED]

[REDACTED]

[REDACTED]



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 17

[REDACTED]

[REDACTED]

[REDACTED]

EFFECTIVE: 04/08/96

10-8 STORED WIRE AND ELECTRONIC COMMUNICATIONS AND  
TRANSACTIONAL RECORDS ACCESS

Title 18, USC, Section 2703, sets forth the procedural requirements that the Government must meet in order to obtain access to electronic communications in storage and related transactional records, including telephone toll records.

EFFECTIVE: 01/22/90

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 18

10-8.1 Contents of Electronic Communications in Electronic Storage

The statute draws a distinction between contents of electronic communications that have been in storage for 180 days or less, and those that have been stored for a longer period of time. This distinction is based on the belief that while the contents of a message in storage should be protected by Fourth Amendment standards, as are the contents of a regularly mailed letter, to the extent that the record is kept beyond six months, it is closer to a business record maintained by a third party for its own benefit and, therefore, deserving of a lesser standard of protection. A distinction is also made for contents of electronic communication in a remote computing service.

(1) 180 days or less - A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication that is in electronic storage in an electronic communications system for 180 days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent state warrant (Title 18, USC, Section 2703(a)).

(2) More than 180 days - For contents of an electronic communication that has been stored for more than 180 days, a governmental entity may use any of three alternative means of access, depending on the notice given to the subscriber, or customer. The government may, without providing any notice to the subscriber, obtain a state or federal search warrant based upon probable cause (Title 18, USC, Section 2703(b)(1)(A)). If the government chooses to give notice to the subscriber, it may obtain access to the records by using either a grand jury, administrative, or trial subpoena authorized by a federal or state statute (Title 18, USC, Section 2703(b)(1)(B)(i)), or a new statutory court order based upon specific and articulable facts showing that there are reasonable grounds to believe that the contents of stored electronic communications are "relevant and material to an ongoing criminal investigation" (Title 18, USC, Section 2703(b)(1)(B)(ii) and (d)). This court order, like a court order for a pen register or trap and trace, may be obtained from a "court of competent jurisdiction" which includes "a district court of the United States (including a magistrate of such a court) or a United States Court of Appeals." The required notice may be delayed pursuant to Title 18, USC, Section 2705.

(3) Contents of electronic communications in a remote computing service - Access to the contents of electronic

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 19

communications is governed by Title 18, USC, Section 2703(b) and the means of access available are the same as those mentioned above for communications stored for more than 180 days. However, it is unclear whether communications stored in a remote computing service for less than 180 days are governed by Title 18, USC, Section 2703(a), that is, that such communications can be obtained ONLY by a federal or state search warrant based upon probable cause. The Department of Justice has urged United States Attorneys to argue that government access to the contents of an electronic communication held by a remote computing service does not require a search warrant during the first 180 days. Questions relating to this area should be directed to the Investigative Law Unit, FBIHQ.

EFFECTIVE: 10/23/95

10-8.2 Access to Transactional Information

(1) Telephone Records (See MIOG, Part II, 21-23(9).)

(a) Criminal and Civil Matters - Access to telephone billing records and other transactional records (not including the contents of communications) is governed by Title 18, USC, Section 2703. Specifically, the disclosure of a record or other information pertaining to a subscriber to a governmental entity is permitted only when the governmental entity:

1. obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent state warrant;

2. obtains a court order for such disclosure under Title 18, USC, Section 2703(d); or

3. has the consent of the subscriber or customer to such disclosure.

In addition to these methods, an administrative subpoena authorized by a federal or state statute, or a federal or state grand jury, or trial subpoena may be used to obtain basic subscriber information such as: "the name, address, telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to or customer of such service and the types of services the subscriber or customer utilize(s)." Title 18, USC, Section

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 20

| 2703(c) (1) (C). |

The Department of Justice has, however, advised that it is a misuse of the grand jury to utilize the grand jury as an investigative aid in the search for a fugitive in whose testimony the grand jury has no interest. Therefore, grand jury subpoenas for witnesses or records, including telephone|billing|records, should not be requested in federal fugitive investigations. (See Part II, Section 2-9.8, of this manual for limited situations in which courts have recognized that grand jury efforts to locate a fugitive are proper.) Where the telephone|billing|records being sought are those of a member of the news media, approval of the Attorney General is required. (See MAOP, Part II, Section 5-7.1 entitled "Investigations Involving Members of the Media.")

(b) National Security Cases - See Foreign Counterintelligence Manual, |Introduction, |Section|1. |

(c) Notification to Telephone Subscriber

Criminal and Civil Matters - Many electronic communication service providers of long distance telephone service will automatically notify a subscriber that his/her records have been released to law enforcement unless the SAC certifies that such notification would prejudice an investigation. The certification period is 90 days, after which many electronic communication service providers will automatically notify the subscriber of the release within five days unless there is a recertification. Each recertification extends the nondisclosure period for an additional 90 days. At the conclusion of the final recertification period, the subscriber will, within five days, be notified of the record release. Each SAC must ensure appropriate administrative devices are in effect to provide for the initial certification where required and recertification prior to the termination of the preceding 90-day period where a continuing need for nondisclosure exists.

(2) |On-line Computer Network Records

(a) Records of on-line electronic communications and electronic mail (e-mail) transmissions, when they reveal more than basic subscriber records (see Title 18, USC, Section 2703(1) (c) (C) e.g., the named addressee, the topic of or the forum connected with the communication, etc.), are no longer available to law enforcement agencies pursuant to subpoena. Such information may be obtained only through the use of a court order under Title 18, USC, Section 2703(d), a warrant, or the consent of the subscriber or customer (Title 18,

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 21

USC, Section 2703(c)).

(b) To obtain a 2703(d) court order, the application must state "specific and articulable facts showing that there are reasonable grounds to believe that the contents of, transactional records of, or other information sought regarding stored electronic communications are "relevant and material to an ongoing criminal investigation."

(3) Video Tape Rental or Sales Records

The Video Privacy Protection Act of 1988 amended Chapter 121 of Title 18 "Stored Wire and Electronic Communications and Transactional Records Access" by adding a new section (redesignation of section 2710) governing the disclosure of video tape rental or sales records. It makes the unauthorized disclosure of records by any person engaged in the rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials unlawful and provides an exclusionary rule to prohibit personally identifiable information otherwise obtained from being admissible as evidence in any court proceeding.

(a) The new section defines personally identifiable information as "information which identifies a person as having requested or obtained specific video material or services . . . ." The disclosure of this information to law enforcement is permitted only when the law enforcement agency:

1. Has the written consent of the customer; or
2. obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State Warrant;
3. a grand jury subpoena;
4. a court order (a court order shall issue only upon prior notice to the consumer/customer).

(b) The disclosure of merely the name, address, and telephone number of customers of a video tape service provider, when the information being sought does not identify the customer as having requested or obtained specific video materials or services, may be made to law enforcement without compulsory process or the prior opportunity to prohibit such disclosure by the customer.

This type of information was specifically not included in the

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 22

definition of "personally identifiable information" (that type of information protected by the Video Privacy Protection Act of 1988) to allow law enforcement to obtain information about individuals during routine investigations such as neighborhood investigations.

(c) No separate disclosure procedure was provided for National Security cases.

EFFECTIVE: 10/23/95

---

10-9 ELECTRONIC SURVEILLANCE (ELSUR) PROCEDURES AND REQUIREMENTS

(1) Electronic surveillance is one of the most effective and valuable investigative techniques utilized in both criminal and national security investigative matters. To protect the use of this technique, the administrative and management controls contained in this section will receive the same meticulous oversight as does the informant program. Unless otherwise noted, it will be the responsibility of the case Agent and his/her supervisor to ensure compliance with these instructions. It should be clearly understood that the use of electronic surveillance requires (a) administrative or judicial authorization prior to its use, and (b) contact with the field office ELSUR support employee to coordinate all necessary recordkeeping, and (c) consultation with the Technical Advisor (TA) or a designated Technically Trained Agent (TTA) to determine feasibility, applicable technique, and the appropriate equipment.

(2) The procedures and requirements for ELSUR recordkeeping, control of evidentiary-type materials, and approval for use with regard to national security investigations are addressed in the Foreign Counterintelligence Manual.

EFFECTIVE: 04/24/89

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 23

10-9.1 Definitions

- (1) Electronic Surveillance - The aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device (Title 18, USC, Section 2510 et seq.).
- (2) ELSUR Indices - An alphanumerical index card system maintained at FBIHQ and each appropriate FBI field office containing the names of all individuals or entities, all locations and all facilities for which electronic surveillance has been sought by the FBI in a court order. It also identifies those individuals who have been participants in a conversation monitored or overheard during the course of an FBI electronic surveillance; and those who own, lease, license, or otherwise hold a possessory interest in property subjected to an electronic surveillance conducted by the FBI.
- (3) ELSUR Cards - 3-x-5-inch cards which comprise the ELSUR indices.
- (4) Principal Cards - 3-x-5-inch cards maintained in the ELSUR indices containing the true name or best-known name of all named interceptees identified in any application filed in support of court authorized Title III electronic surveillance. (See 10-9.12(1).)
- (5) Proprietary Interest Cards - 3-x-5-inch cards maintained in the ELSUR indices identifying the entity(s) and individual(s) who own, lease, license, or otherwise hold a possessory interest in locations subjected to electronic surveillance authorized under Title III.
- (6) Overhear Cards - 3-x-5-inch cards maintained in the ELSUR indices containing the true name or best-known name of individuals (including non-U.S. persons, Special Agents, assets, informants, cooperating witnesses, etc.) who have been reasonably identified by a first name or initial and a last name as having participated in conversations intercepted during the conducting of an electronic surveillance. (See 10-9.10 and 10-10 for further details.)
- (7) Blue ELSUR Index Cards - 3-x-5-inch cards, blue in color, used for preparing Principal, Proprietary Interest and Overhear cards in Title III matters. All ELSUR cards relating to Title III are blue in color.
- (8) White ELSUR Index Cards - 3-x-5-inch cards, white in color, used for preparing Overhear cards in consensual monitoring

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 24

matters.

(9) Source - With regard to ELSUR matters, the word "source" refers to the technique (microphone, telephone, body recorders, etc.) employed to conduct the electronic surveillance. In Title III matters, the "source" is the control number assigned; and in consensual monitoring matters, the "source" will be the control number assigned or the word "consensual."

(10) Title III Electronic Surveillance - The aural or other acquisition of the contents of any wire, electronic or oral communication pursuant to a court order obtained under the provisions of the Omnibus Crime Control and Safe Streets Act of 1968 (Title 18, USC, Section 2510 et seq.) for offenses set forth in Title 18, USC, Section 2516.

(11) Consensual Monitoring - The interception by an electronic device of any wire or oral communication wherein one of the parties to the conversation has given prior consent to such monitoring and/or recording.

EFFECTIVE: 04/24/89

10-9.2 Instructions for Maintaining ELSUR Indices

(1) The FBI has an obligation to totally retrieve the authority, contents and resulting use of material acquired regarding all persons targeted, monitored, or who otherwise hold a possessory interest in property subjected to electronic surveillance by this Bureau. In order to fulfill this obligation, it is the responsibility of each field office to comply with these instructions so that any electronic surveillance can be recalled from the files of the FBI.

(2) Indexing procedures in ELSUR matters will be the same as those set forth in the "Index Guide" which is available in each field office through the File Assistant/ELSUR support employee. All offices utilizing electronic surveillances will maintain one ELSUR index and prepare two copies of the appropriate-type ELSUR card, one for forwarding to FBIHQ and one for inclusion in the field office ELSUR indices. Each card filed in the field office ELSUR indices will be date-stamped to reflect the month, day and year the card was filed. Cards prepared in the name of an individual will be filed in alphabetical order according to the last name. Names of businesses, organizations, etc., will also be filed in alphabetical order.

Sensitive  
PRINTED: 02/18/98



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 25

Proprietary Interest cards cross-referencing telephone and vehicle identification numbers will be filed in a separate section within the ELSUR indices in numerical order according to the last three digits of the number. Should the last three digits be identical with any already in file, proceed to the next digit to the left. Addresses will be filed according to the name of the street; numbered streets will be spelled out, and in both cases will be filed in alphabetical order in a separate section within the ELSUR indices. In the event an address contains two street names, an appropriate card will be made for filing by each street name.

(3) The ELSUR indices will be maintained in a securely locked cabinet and will operate exclusively under the supervision of the field office ELSUR coordinator or the support employee designated to assist the coordinator. Access to the ELSUR index must be restricted to an absolute need-to-know basis.

(4) In the event any ELSUR index card within the ELSUR indices in any given field division is classified according to existing Executive order instructions to protect information involving national security, the ELSUR index of that field division must be classified at the level of the highest classification of any material contained therein. Any information retrieved as a result of a search of the ELSUR index must be reviewed for proper classification prior to internal FBI dissemination and/or subsequent release.

(5) The assistant ELSUR coordinator will conduct an annual review of the ELSUR indices to locate and correct misfiled cards, duplications, and subsequent overhears. Particular attention will be given to Proprietary Interest cards and Principal cards to ensure each item is complete where necessary. As this review is completed, an index card will be inserted at the front of each drawer within the index and will show the date the review was completed and the initials of the employee who conducted the review.

EFFECTIVE: 02/16/89

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 26

10-9.3 Requests for ELSUR Checks

(1) Upon submitting a request to FBIHQ for an electronic surveillance indices check, it is necessary to indicate in each request the reason why the information is being sought, such as whether the sought after ELSUR information will be used for preparation of a Title III affidavit, for an investigative lead, or for other purposes.

(2) Field office personnel handling ELSUR checks should also note that per U.S. Attorney's Manual, Title 9, Section 9-7.000, all requests for search of electronic surveillance records under a defense claim pursuant to Title 18, USC, Section 3504, or Federal Rules of Criminal Procedure, Rule 16, or for other trial-related reasons, must be directed by the Government trial attorney to the Department of Justice, Criminal Division, Attention: Legal Support Unit, Office of Enforcement Operations, Telephone Number FTS [REDACTED] b2  
All assertions on behalf of the United States must be made by the Attorney General or Attorney General's designee. In the event a Government trial attorney requests an ELSUR check, the attorney should be advised of the instructions referred to above in the U.S. Attorney's Manual.

EFFECTIVE: 04/18/85

10-9.4 ELSUR Searching Procedures

(1) In connection with White House inquiries, requests under the Freedom of Information/Privacy Acts (FOIPA), discovery motions, U.S. District Court orders, and other lawful motions emanating from the courts, the Department of Justice directs inquiries to FBIHQ regarding possible electronic surveillance coverage of witnesses, defendants, or attorneys involved in Federal court proceedings. In order to accurately respond to such requests, field offices receiving instructions from FBIHQ to conduct a search of the ELSUR index and general office indices should search the name as shown, as well as aliases, variations in spelling, combinations and contractions, the extent of which is determined by the searching employee. All combinations searched must be shown on the incoming communication or an attached search slip so that the extent of the index search is readily apparent.

(2) An individual who has been party to a conversation intercepted by electronic surveillance may frame a request under the

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 27

FOIPA to include a search of the ELSUR indices. Such would require close coordination between FBIHQ and the field division which may have submitted ELSUR indices cards identifiable with the requester.

(3) This process of coordination will generally be initiated by an FOIPA Section airtel to the appropriate field division when the FOIPA request is received for processing. This airtel will request review of field office ELSUR records to determine if the individual monitored is identical to the requester and if there are additional instances of monitoring. FBIHQ ELSUR Index may not have previously alerted the FOIPA Section that the individual was monitored in a consensual or Title III electronic surveillance investigation.

(4) Where the overheard is recent in date, it is possible that the consensual electronic surveillance in question relates to a pending investigation or a covert operation not yet disclosed. The pending character of this investigative matter would not be evident from the FBIHQ ELSUR Index records. This pending status governs FOIPA Section processing of the ELSUR request and the FOIPA Section must be made aware of the status to ensure that the fact of an overheard will not be prematurely disclosed to the requester.

(5) Therefore, in responding to an FOIPA Section airtel relating to consensual monitoring ELSURs, the field division should always advise if the ELSUR coverage in question is still pending or a covert operation not yet disclosed.

(6) The ELSUR index should also be searched for any telephone numbers and addresses provided in the departmental request. All indicated files resulting from the search should be thoroughly reviewed for information relative to electronic surveillance.

EFFECTIVE: 04/18/85

10-9.5 Transmitting ELSUR Material to FBIHQ

(1) ELSUR index cards will be submitted, utilizing Form FD-664. This is a preprinted form directed to the ELSUR Index at FBIHQ. FD-664 requires the submitting field office to fill in blanks on the FD-664 reflecting the exact number of index cards submitted, the exact field office case title and file number and the technique utilized for the ELSUR. An inventory is required on the FD-664 indicating the identity of the ELSUR index cards submitted; therefore, list the name(s), entity(s), address(s), telephone number(s), and

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 28

vehicle identification number(s) indexed on the top line of each card enclosed. Lengthy submissions may be reflected by addenda to the form. Further, the FD-664 may be utilized for noncriminal matters. If utilized for noncriminal matters, the proper classification should be affixed to the form. The original and one copy of the FD-664, as well as accompanying enclosures, will be inserted in a plain brown envelope, sealed and clearly marked:

Director, FBI  
ELSUR Index  
FBIHQ

and submitted to reach the Bureau within the time frame allotted.

(2) Unless instructed to the contrary, responses to ELSUR surveys and related correspondence will be transmitted to the Bureau by airtel to: Director, FBI, Attention: ELSUR Index. This airtel should be entitled "ELSUR." The original and one copy of the transmittal airtel as well as accompanying enclosures will be inserted in a plain brown envelope sealed and clearly marked: Director, FBI, ELSUR Index, FBIHQ. This airtel will be submitted to reach the Bureau within the time frame allotted the specific type of material being forwarded and within Bureau deadline.

(3) When a court-ordered surveillance is authorized, installed, extended, or when a noncriminal matter installation is made or approved, an FD-664 should be submitted to FBIHQ. This does not preclude submission of a teletype or other expeditious communication to the appropriate substantive investigative section in criminal or noncriminal matters pertaining to emergency authorizations of both court-ordered or noncourt-ordered matters. All communications should be classified according to material contained within the communication. All communications should contain the field office case title and complete file number. Any communications concerning expeditious authorization and/or installation should contain also the name(s) of target(s), address(s) telephone number(s), source number of the installation or consensual monitoring number and dates of authorization, installation, extension and expected termination.

EFFECTIVE: 06/18/87

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 29

10-9.6 Retention of ELSUR Files and Related Records

On January 10, 1980, Judge Harold H. Greene, U.S. District Court, District of Columbia, issued a preliminary injunction to suspend all records destruction programs. Since that time, this order has been modified somewhat; however, these modifications did not include ELSUR materials. Until otherwise advised by FBIHQ, all originals and copies of original tapes, logs, transcripts, records, files and communications reflecting any ELSUR information relating to Title III matters, criminal intelligence matters and consensual monitoring matters will be retained.

EFFECTIVE: 06/18/87

10-9.7 Marking File Cover "ELSUR"

To ensure certain files are retained beyond the established file destruction period, a check mark will be placed on the ELSUR line or "ELSUR" will be stamped on the case file covers of those files containing the "results" or the "products" of electronic surveillance on every current, every preceding, every subsequent and every Sub volume to the file even though the product of the electronic surveillance may have been taken from another file or furnished by another office.

EFFECTIVE: 12/10/93

10-9.8 Preservation of Original Tape Recordings (See MIOG, Part II, 10-9.8.1(1), 10-10.5.1(2)(c); LHBSA, 7-14; FCIM, Introduction, 1-2.6.3(10).)

All original criminal ELSUR-taped recordings will be placed in an FD-504 (Chain of Custody - Original Tape Recording Envelope), sealed and retained in a modified steel wardrobe-type cabinet, security-approved container, or metal file cabinet equipped with a bar-lock device, hasp or other security-approved lock unless, under Title III, the authorizing judge has directed to the contrary. These cabinets are to be housed in a limited or restricted access location to ensure against unauthorized access in order to overcome any claim that the ELSUR tape was altered or distorted while in the

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 30

possession of the FBI and to assure the chain of custody. (See 10-9.6 for current rules regarding the retention of taped recordings. In matters involving national security refer to the Foreign Counterintelligence Manual for instructions regarding the handling of national security taped recordings.)

EFFECTIVE: 12/21/94

10-9.8.1 FD-504 (Chain of Custody - Original Tape Recording Envelope) (See Legal Handbook for Special Agents, 7-14.)

(1) ALL original tape recordings (including closed circuit television recordings) maintained as a part of a permanent record of the FBI, as well as those sealed by the U.S. District Judge, should be placed in an FD-504 envelope, maintained as evidence, and stored as instructed above in Section 10-9.8 of this manual.

(2) The procedures for filling out the FD-504 are as follows:

(a) File Number - Enter the substantive case file number to which the tape recording relates and include the 1B (Evidence) number.

(b) Tape Number - Enter the sequential number given the tape recording enclosed.

(c) Agent Supervising Interception - Enter the name of the Agent (or other Bureau employee) who removes the tape from the recording device after the recording is made; or who first receives custody of the original tape after the recording is made and the tape is being surrendered for retention.

(d) Title III Court-Order or FISA Court-Order Control Number: Mark appropriate space to indicate if the ELSUR is authorized under Title III or under the Foreign Intelligence Surveillance Act (FISA) of 1978, and enter the control/symbol number assigned.

(e) Consensual ELSURs - Mark appropriate box to indicate Consensual Monitoring (CM) telephone or nontelephone and any CM number assigned.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 31

(f) In instances wherein the original tape recording enclosed in an FD-504 envelope is not a court-ordered or consensual ELSUR, mark the appropriate box to identify the origin of the tape enclosed, (i.e., Volunteered Tape-Not FBI ELSUR; Interview; other).

(g) Interception: Date and Place - Enter date and place (city/town and state) where intercept occurred.

(h) Tape Removed From Equipment - Enter date and time the tape was removed from the recording device.

~~(i) Identity of Persons Intercepted, If Known -~~

Enter "See Log" for all court-ordered ELSURs (those authorized under Title III and under the FISA of 1978). For warrantless ELSURs (Consensual Monitoring) enter the true name or best known name of ALL individuals (including the consenting party) identified as having been overheard.

CHAIN OF CUSTODY

(j) Accepted Custody - Signature of the first person accepting custody of the recording (Agent supervising the intercept and/or any others taking custody of the contents of the FD-504).

(k) Released Custody - The released custody column should show the signature of the last person accepting custody and then releasing custody to the next person. The last name exhibited as accepting custody would normally be the individual that places the evidence in the tape storage facility and thus releases custody, by signature, to the tape storage facility for permanent storage. (See Title III Section of the ELSUR Working Guide, page 44).

(3) In sealing the FD-504 envelope, the flap should be moistened, then sealed. The date the envelope is sealed and the initials of the employee sealing the envelope should be affixed on the flap at the point where the end of the flap meets the envelope. Yellow transparent preprinted "evidence tape" should then be placed atop the seam of the flap and overlapping to the other side of each edge of the envelope, as shown in the Title III Section of the ELSUR Working Guide, pages 44 and 45.

(4) In those situations involving interoffice travel and ELSUR usage, i.e., body recorder, ensure original recordings are entered into chain of custody as evidence within 10 days of the receipt of the recording, as required in the Manual of Administrative Operations and Procedures, Part II, Section 2-4.4.4. All original

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 32

tapes are to remain in the field office where first entered as evidence. If tapes are entered into the recordkeeping system of the host office (the office wherein the tape was made), the recordings will remain in the custody of the host office. ELSUR indexing will be done by the office where the tape recordings are entered as evidence, and, if appropriate, host office copies of the recordings will be made and forwarded to other concerned field offices by the custodial offices.

(5) If, during the conduct of an ELSUR, the recording device fails to operate or malfunctions and the tape is found to be blank or contains only portions of the conversation, the tape is to be retained in an FD-504 envelope as described herein.

EFFECTIVE: 10/16/96

10-9.9 Recordkeeping Procedures for ELSUR Information Generated Through Joint FBI Operations

(1) In joint FBI operations with other Federal, state and local law enforcement agencies wherein electronic surveillance is conducted through a Title III installation, the agency which prepares the affidavit, application and order seeking the authority will assume all responsibility for ELSUR indexing and recordkeeping. The fact that the investigation is a joint operation will be stated in the affidavit and application for the court order and will specify which agency is lending support to the other.

(2) Accordingly, if an outside law enforcement agency prepares the affidavit, application, and order in a Title III criminal matter in which the FBI is lending investigative support, that agency is responsible for the proper maintenance of all transcripts and tapes resulting from the Title III installation. In such case, that agency is also responsible for the preparation of electronic surveillance index cards and none would be prepared for inclusion in the FBI electronic surveillance indices.

(3) With regard to consensual monitoring, the agency that obtains authorization for consensual monitoring will assume all responsibility for the necessary ELSUR indexing and recordkeeping. See 10-10.2 or 10-10.3.

Sensitive  
PRINTED: 02/18/98



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 33

EFFECTIVE: 10/18/88

10-9.10 Electronic Surveillance - Title III Criminal Matters  
(See MIOG, Part I, 9-7.2; Part II, 10-3, 10-9.1(6) &  
10-10.9.1 (4) (b).)

An FD-669, Checklist-Title III (Criminal Matters) form, is to be executed, serialized and retained in a separate sublettered file to the case file. One form is to be prepared for each application filed in each investigation. Every item contained thereon is to be initialed as completed and, where appropriate, will show the serial number of the communication prepared that ensures the requirement has been met.

(1) Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title 18, USC, Sections 2510-2521) provides a legislative basis with carefully constructed controls, requirements, and limitations for the judicial authorization of electronic surveillance techniques in certain major violations, including, but not limited to:

(a) Organized crime activities such as certain gambling offenses, racketeering, extortionate credit transactions and use of interstate commerce facilities in the commission of murder for hire;

(b) Murder, kidnapping, robbery or extortion prosecutable under Title 18, U.S. Code;

(c) Presidential assassination, kidnapping, or assault;

(d) Obstruction of justice;

(e) Interference with interstate commerce by violence or threats of violence;

(f) Interstate transportation of stolen property, theft from interstate shipment, and interstate travel to incite a riot;

(g) Espionage, sabotage, treason and the illegal acquisition or disclosure of atomic energy information; (See (2).)

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 2/23/98 BY SP5/SC/JAI

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 34

- (h) Sexual exploitation of children;
- (i) Interstate transportation or receipt of stolen vehicles;
- (j) Hostage taking;
- (k) Mail fraud;
- (l) Fugitive from justice from an offense described in Title 18, USC, Section 2516(1);
- (m) Certain firearms violations;
- (n) Obscenity;
- (o) See Title 18, USC, Section 2516, for a complete listing of applicable violations.

(2) With respect to the types of investigations listed in item (g) above, which might be the act of an agent of a foreign power, consideration should be given to obtaining electronic surveillance according to the provisions of the Foreign Intelligence Surveillance Act of 1978 (FISA) (Title 50, USC, Section 1801 ET SEQ.). It is generally accepted that the provisions of FISA afford greater security to the government's case, as there are detailed security precautions incorporated into the entire process. While obtaining electronic surveillance pursuant to FISA may be more difficult than a Title III surveillance in those instances where foreign powers may be involved, it should be the preferred method. If electronic surveillance pursuant to FISA is determined to be the preferred method in a particular investigation, concurrence of the USA is not required, as this function will be coordinated by FBIHQ with the appropriate Department of Justice office. (See National Foreign Intelligence Program Manual, Appendix 4-1.2, for procedures in obtaining a FISA court order.)

(3) Title III Applications - Approval Levels

(a) The initial phase in the stringent administrative approval process of Title III applications commences at the field level with the review and approval of the Title III affidavit by field office supervisory personnel, the Chief Division Counsel (CDC) and the concurrence of the respective USA or Strike Force Attorney. Review by the CDC must be documented by completing the "CDC Title III Log/Checklist" for submission along with the

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 35

affidavit to FBIHQ. The CDC in each field office is completely familiar with the statutory and procedural requirements for electronic surveillance, and must be consulted whenever a Title III is being considered.

(b) FBIHQ's responsibilities towards requests for court-ordered electronic surveillances are that of case supervision and executive approval. With regard to executive approval, the management level at which requests for Title III electronic surveillances can be approved is dependent upon the circumstances surrounding the request. FBIHQ has recognized seven specific situations that have been characterized as "sensitive issues." The following five (5) sensitive issues or circumstances require the approval of a Deputy Assistant Director or higher from the Criminal Investigative Division (CID) or National Security Division (NSD) as appropriate:

1. applications requesting Title III interceptions based upon "relaxed specificity" (i.e., applications in which the requirement to specify those facilities from which, or the place where, the communication is to be intercepted has been eliminated--so called "roving" interceptions) under provisions of Title 18, USC, Section 2518(11) (a) and (b);

2. situations involving significant privilege issues or First Amendment concerns (e.g., attorney-client privilege or other privileged conversations, or interception of news media representatives);

3. situations involving significant privacy concerns (e.g., interceptions of conversations in a bedroom or bathroom, etc.);

4. applications concerning Domestic Terrorism, International Terrorism, or Espionage cases;

5. in any other situation deemed appropriate by either the Assistant Director, CID, or Assistant Director, NSD.

The following TWO (2) instances require the approval of the Director or the Acting Director when conducting sensitive Title III applications:

1. "emergency" Title III interceptions (i.e., interceptions conducted prior to judicial approval under provisions found in Title 18, USC, Section 2518(7));

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 36

2. the anticipated interception of conversations of members of Congress, federal judges, high-level federal officials; and high-level state executives and members of a state judiciary or legislature.

ALL requests for electronic surveillance which involve one of the above "sensitive issues" must be reviewed by the Office of the General Counsel (OGC) prior to approval.

NONSENSITIVE Title III applications for electronic surveillance of wire and oral communications and of electronic communications NOT involving ~~digital display paging devices~~ may be approved at the appropriate FBIHQ Section Chief level in the CID.

Title III applications for authorization to intercept electronic communications over a ~~digital display pager~~ do NOT require FBIHQ review and approval, but may proceed with SAC approval. (See MIOG, Part II, 10-10.11.1(2)(b).)

In any instance where there are legal questions/concerns that cannot be resolved through discussions with reviewing officials at the Department of Justice, CID supervisors and/or executives will forward applications involving such issues to OGC for their review, advice and recommendations.

(c) Thereafter, with the approval of the Attorney General, or Attorney General's designee, the USA or the Strike Force Attorney shall apply to a federal judge of a competent jurisdiction for a court order authorizing the interception of communications relating to the specified offenses listed in Title III (Title 18, USC, Section 2516). Judicial control, however, does not cease with the signing of a court order authorizing the interception of communications but continues into the operational phase of the electronic surveillance--installation, monitoring, transcribing and handling of tapes. In addition, a cover electronic communication is to be sent to FBIHQ with a copy of each periodic report prepared for the prosecuting attorney and filed with the court. This report is to be submitted to FBIHQ the same day or next workday after the periodic report is filed with the court.

(d) An EXTENSION order may be sought to continue monitoring beyond the initial 30-day period without a lapse in time. When a break in coverage has occurred, a RENEWAL order may be sought to continue monitoring the same interceptees or facilities identified in the original authorization. The affidavit and application in

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 37

support of an extension or renewal must comply with the same requirements as an original Title III application, including approval of the Attorney General or designee.

Except as explained below, extensions and renewals which occur within 30 days of the original Title III order do NOT require review by FBIHQ. After a lapse of more than 30 days, DOJ requires review by FBIHQ and a memorandum requesting renewed electronic surveillance. There may be situations when particularly unusual circumstances dictate that the FBI adopt an already existing Title III from another federal law enforcement agency. Such a procedure will be approved on a case-by-case basis, and only in exceptional circumstances.

~~Moreover, before the FBI begins or adopts the administration of a~~ Title III pursuant to a court order, the field must obtain FBIHQ approval. Therefore, extensions and renewals within 30 days do NOT require FBIHQ approval ONLY if the Title III in question has already been approved by FBIHQ. In order to ensure compliance with the statutory and procedural requirements, it is imperative that Chief Division Counsel be consulted whenever electronic surveillance is contemplated.

(4) It is essential that the requirements set forth in Title 18, USC, Section 2518, be followed meticulously in the preparation of a Title III application. In addition, it is essential that the following points be covered:

- (a) That the probable cause is current;
- (b) That definite grounds have been established for certifying that normal investigative procedures have been tried and failed or demonstrating why these procedures appear to be unlikely to succeed or would be too dangerous if tried (the courts have made clear that the use of "boilerplate" statements in this respect are unacceptable);
- (c) An attempt has been made to identify the subscriber to the telephone on which coverage is sought, if the name is not that of one of the principals;
- (d) That minimization will be assured, especially when the coverage involves a public telephone booth, a restaurant table, or the like;
- (e) That the premises to be covered are described fully, including a diagram, if possible, in requests for microphone installations (although no surreptitious entries are to be conducted

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 38

for the purpose of obtaining such data), (see 10-9.10(6) below);

(f) That upon consideration of preparing an affidavit for coverage under Title III, the field office forward an electronic communication to FBIHQ, under case caption, setting forth by separate subheading the SYNOPSIS OF OVERALL INVESTIGATION, PRIORITY OF THE INVESTIGATION WITHIN THE DIVISION, ANTICIPATED MANPOWER REQUIREMENTS AND WHAT OUTSIDE SUPPORT, IF ANY, WILL BE NEEDED, a SYNOPSIS OF PROBABLE CAUSE JUSTIFYING TITLE III APPLICATION, the PROSECUTIVE OPINION of the U.S. Attorney, and CHARACTERIZATION OF THE INTERCEPTES;

(g) That a request for an ELSUR search of all office records be submitted, in writing, to the office ELSUR File Assistant (EFA) within 45 days prior to the submission of the affidavit to FBIHQ. The request should identify the substantive case title, to include the violation and field office file number. It should state the request is being submitted in anticipation of Title III ELSUR coverage and list the following: (1) person(s), (2) facility(s), (3) place(s) and, if appropriate, (4) vehicle identification number(s), etc., under consideration in order to identify prior applications. The EFA will conduct a search of the ELSUR Automated Records System (EARS) database requesting "all office records." Only the Principal, Proprietary Interest, and Intercept records contained in the EARS database, which relate to unclassified criminal matters, should be printed in their entirety, attached to the search request, and furnished the requestor. No information relating to court-ordered ELSURs conducted pursuant to the Foreign Intelligence Surveillance Act or information relating to consensual monitorings conducted pursuant to Attorney General Guidelines for FBI Foreign Intelligence Collections and Foreign Counterintelligence Investigations should be printed or provided to the requestor. It is the responsibility of the requestor in the office seeking a new court order to follow up the results of the search. Contact must be made with those offices identified as having filed previous applications to the court to obtain facts required for inclusion in the affidavit being prepared.

(h) Where extension orders are sought naming NEW person(s) (principals/targets), facility(s) or place(s), an ELSUR search must be conducted on the newly added principals/targets, prior to submission of the extension affidavit to the DOJ. Where extension orders are sought naming the same principals/targets, facilities, or places specified in the initial affidavit submitted to FBIHQ, a "recheck" of the EARS will be conducted for the purpose of updating the search. The "recheck" will be conducted for all extensions sought 90 days following the filing of the initial application.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 39

(i) Requests for ELSUR searches which relate to Title 21, USC violations, must be searched through the Drug Enforcement Administration (DEA), Washington, D.C. This will be accomplished by the FBIHQ ELSUR index for all search requests which relate to 245 violations. The need for an ELSUR search of the DEA records for any other violation must be specifically requested through the office EFA at the time the ELSUR search request is submitted. All pre-Title III ELSUR searches conducted will be transmitted to FBIHQ ELSUR index automatically via the EARS. Headquarters will forward the request to the DEA, Washington, D.C., and provide a response to the requesting office. Appropriate documentation confirming the conduct of all pre-Title III searches must be serialized and filed in the substantive case file or the corresponding ELSUR subfile to the case file. Documentation may be in the form of an electronic communication, teletype, or search slip. Requests for a search of the ELSUR index received from any outside agency or department are to be referred to the ELSUR subunit at FBIHQ.

(5) See Title 18, USC, Section 2518 for a complete listing of the statutory requirements (procedure for interception of Title III);

(6) Where it is necessary, prior to issuance of a court order, to survey property or premises to determine the feasibility of installation of wire or oral communication intercepting devices, or other electronic surveillance devices such as beepers and closed circuit television cameras, the survey shall not exceed lawful activity, i.e., no entry or other intrusion into an area where a reasonable expectation of privacy exists may be made absent consent of the proper party. (See (4) (e) above.)

(7) In matters involving the use of Closed Circuit Television (CCTV) in conjunction with a Title III electronic surveillance, refer also to Part II, Section 10-10.1 & 10-10.9 of this manual.

(8) Roving Interceptions. One of the most significant additions to Title 18, USC, Section 2518 brought about by the Electronic Communications Privacy Act of 1986 concerns the specificity required in the description of the place where, or the telephone over which, electronic surveillance is to be conducted. The original law required that the application for, and the order authorizing, an electronic surveillance request indicate the "particular" facility or place in which the interception was to occur. The new law contains an exception to the particularity requirement and, in effect, allows an

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 40

interception order to target a specific person rather than the specific telephone or premises that person might use. The amendments establish two similar rules to govern the interception of "oral communications" and "wire or electronic communications" where the target facility need not be identified with specificity before the interception order is obtained (Title 18, USC, Section 2518(11)).

(a) With respect to "oral communications," the application must contain a full and complete statement as to why the ordinary specification requirements are not practical. The application must also identify the person committing the offense and whose communications are to be intercepted. The judge must then make a specific finding that the ordinary specification rules are not practical under the circumstances (Title 18, USC, Section 2518(11)(a)). Examples of situations where ordinary specification rules would not be practical include cases in which suspects meet in parking lots or fields or move from hotel room to hotel room in an attempt to avoid electronic surveillance. In such cases, the order would allow law enforcement officers to follow the targeted individual and engage in the interception once the conversation occurs (Title 18, USC, Section 2518(12)).

(b) The provision concerning "wire or electronic communications" is similar to that governing oral communications. The application must specifically identify the person committing the offense whose communications are to be intercepted. The application must also show, however, that the person committing the offense has demonstrated a purpose to thwart interception by changing facilities. In these cases, the court must specifically find that such purpose has been evidenced by the suspect. An example of a situation that would meet this test would be the subject who moves from phone booth to phone booth numerous times to avoid interception (Title 18, USC, Section 2518(11)(b)).

b2  
L7E

(c) With respect to both oral and wire or electronic communications, the approval of the Attorney General, Deputy Attorney General, Associate Attorney General, Assistant Attorney General or an Acting Assistant Attorney General is required before a relaxed specificity order is sought. Approval by a Deputy Assistant Attorney General in the Criminal Division, which is authorized for all other interceptions, is not sufficient for this type of application.

(d) The government cannot begin the interception until the facilities from which, or the place where, the communication is to be intercepted is determined by the agency implementing the order (Title 18, USC, Section 2518(12)). Congress also intended that



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 41

the actual interception not commence until the targeted individual begins, or evidences an intention to begin, a conversation. It was not intended that the relaxed specificity order be used to tap a series of telephones, intercept all conversations over those phones, and then minimize the conversations recorded as a result. This provision puts the burden on the investigatory agency to determine when and where the interception is to commence. There is no requirement of notification to the court once the premises or specific phone is identified prior to making the interception; however, a specific place or phone must be identified. Limiting interceptions to specific places once they are determined should satisfy the specificity requirement of the Fourth Amendment.

(e) Obviously, this provision will be a valuable tool in criminal investigations as sophisticated suspects have been quite effective in avoiding electronic surveillance by frequently changing their meeting places and telephones. However, the Fourth Amendment implications involved in this procedure should not be ignored. This is an extraordinary provision and it is the intention of the Department of Justice that it be used sparingly and only in clearly appropriate cases. This provision is not a substitute for investigative footwork; it is not intended that the ordinary showing of probable cause with respect to a specific telephone or location be dispensed with on the theory that the subject is a criminal who engages in criminal conversations wherever he/she goes.

(f) A further consideration, especially in wire or electronic interceptions, is the practical problems faced by the telephone company or other provider of electronic communication services in effecting the interception, complete with leased lines to the government listening post, on extremely short notice. Care has to be exercised to work with the telecommunication companies and to provide them with as much information and notice as possible as far in advance as possible. Telephone companies in particular have expressed great concern about their ability to comply with such orders, which may require action on their part that will strain their ability to assist law enforcement officials in these cases. Congress, at the request of the telephone companies, included a provision in the Act allowing the companies to move the court that has issued a reduced specificity order for the interception of wire or electronic communications to modify or quash the order if the interception cannot be performed in a timely or reasonable manner (Title 18, USC, Section 2518(12)). The key for all concerned is to approach this procedure with care and foresight and to be aware of the practical and legal problems that may arise.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 42

(9) It is also necessary that the post-execution sealing requirements of Title 18, USC, Section 2518(8)(a) be met. Failure to adhere to this requirement could result in suppression of relevant interceptions in the absence of a satisfactory explanation for any delay in sealing. Agents should therefore be prepared to submit the original recordings of all interceptions to the issuing judicial official for sealing immediately at the conclusion of the period of continuously ordered electronic surveillance. In this context, if there is no break in time between the expiration of the original order and any subsequent extensions, Agents may wait until the expiration of the final extension before fulfilling this requirement.

If any delay in making this delivery is anticipated, the Agent supervising the electronic surveillance should document the causes for this delay, i.e., duplication equipment failure, unforeseen manpower allocation priorities, and notify the supervising Assistant United States Attorney or Strike Force Attorney of the anticipated delay. If the supervising Agent anticipates this delay to be any greater than five days from the expiration date of the continuous electronic surveillance, he/she should, through the supervising attorney, within that five-day period obtain an extension of time in which to fulfill the sealing requirements from the appropriate judicial official.

The timely review of Title III electronic surveillance (ELSUR) tapes, CCTV recordings and consensual recordings is crucial to the overall success of a criminal investigation. This review should take place as soon as possible. This is especially true in "crisis" situations, generally defined as "life or death" matters. In those situations, Title III tapes, CCTV recordings and consensual recordings must be reviewed as quickly as possible from the time of the intercept. Pertinent conversations in "crisis" situations must be brought to the attention of supervisory personnel immediately. In all other situations defined as "noncrisis" matters, the tapes should be reviewed promptly, as deemed necessary based upon the exigencies of the investigation. To ensure adherence to this policy, it is incumbent upon the supervisory personnel to establish and follow a systematic policy providing for the appropriate review (articulated above) of all tapes.

(10) Title 18, USC, Section 2518 (5) provides for a 30-day time limitation on Title III interceptions of wire, oral and electronic communications. The 30-day time limitation shall commence at the time and date that the Title III monitoring equipment is activated, regardless of when an actual communication is first intercepted. If the monitoring equipment is not activated within ten days of the signing of the Title III court order, however, the 30-day

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 43

time limitation begins with the eleventh 24-hour period after the order is signed.

EFFECTIVE: 02/28/97

10-9.11 Emergency Provisions, Title III Criminal Matters

(1) In regard to the interception of wire communications or oral communications in which a reasonable expectation of privacy exists, or electronic communications, the Department will generally recognize no exception to their requirement that a warrant first be obtained. However, if an emergency situation exists wherein time does not permit following the warrant process and such electronic surveillance is believed crucial, the Attorney General, Deputy Attorney General, or the Associate Attorney General, under the authority of Title III (Title 18, USC, Section 2518 (7)), can authorize electronic surveillance prior to obtaining a court order. This means, of course, that no SAC or FBIHQ official has the authority on his/her own to authorize interception of wire, oral, or electronic communications, even under emergency circumstances where a human life is in jeopardy. Title 18, USC, Section 2518 (7), which contains the specific requirements for emergency authorization, provides as follows:

"Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that--

"(a) an emergency situation exists that involves--

"(i) immediate danger of death or serious physical injury to any person,

"(ii) conspiratorial activities threatening the national security interest, or

"(iii) conspiratorial activities characteristic of organized crime, that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 44

"(b) there are grounds upon which an order could be entered under this chapter to authorize such interception, may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application."

(2) During normal working hours a field office seeking emergency Title III authorization should advise the appropriate unit of the Criminal Investigative Division (CID), FBIHQ, telephonically of such request, and contemporaneously facsimile a concise written statement of the facts, circumstances and probable cause supporting the request for interception as well as emergency authority. During weekend, holiday, or nighttime hours, requesting field offices should direct emergency Title III telephonic and facsimile communications to the CID duty supervisor who will advise the appropriate CID substantive Unit or Section Chief of the request. The substantive unit will be the point of contact for the field requesting the emergency Title III request and will maintain a log, during normal working hours, pertaining to the progress of the authorization process. During off hours, weekends, and holidays the Emergency Title III request log will be maintained by the CID duty supervisor in the Strategic Information and Operations Center (SIOC).

(3) The grounds upon which an order may be entered (in emergency situations) are limited to violations of those crimes enumerated in Title 18, USC, Section 2516, and to an emergency situation existing that involves immediate danger of death or serious physical injury to any person, conspiratorial activities threatening the national security interest, or conspiratorial activities characteristic of organized crime.

(4) The phrase "conspiratorial activities . . . characteristic of organized crime" is not defined in either the statute or the legislative history. Therefore, what activity meets this definition must be considered on a case-by-case basis. It is

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 45

noted that DOJ has in the past demonstrated a willingness to consider authorizing emergency electronic surveillance on the basis that participants were members of an organized crime group in the traditional sense that the term has been applied. It would seem that, at a minimum, there would have to be evidence of two subjects (exclusive of informants and undercover operatives), conspiring to commit some violation enumerated in Title 18, USC, Section 2516.

(5) With regard to the phrase "conspiratorial activities threatening the national security interest," both the statute and the legislative history are devoid of any definition. Requests from the field for emergency Title III authority may in some cases be examined at FBIHQ to determine any possible applicability that the above statutory language may have to the activity in question. In some cases a determination may be made that the application for electronic surveillance can more appropriately be made under the emergency provisions of the Foreign Intelligence Surveillance Act (Title 50, USC, Section 1805 (e)).

(6) Since Section 2518(7) requires that a written application for electronic surveillance be received by the court from which authorization is being sought within 48 hours after the interception has occurred or begins to occur, preparation of the affidavit should commence contemporaneously with the telephone/facsimile request to FBIHQ. The affidavit should be transmitted by facsimile to FBIHQ as expeditiously as possible to allow for necessary processing by FBIHQ and DOJ, and submission to the appropriate court within the statutory time limit. Field offices may provide assistance to local USAs' offices without facsimile facilities by transmitting the application and proposed order over field office facilities to FBIHQ. These documents will be handcarried along with the affidavit to the DOJ. In accordance with DOJ policy, written application will be made to a court for an order approving the interception, whether or not the interceptions obtained are determined to be fruitful from an evidentiary standpoint. In the event that the need for electronic surveillance evaporates following authorization but prior to the installation and activation of the technical equipment, the submission of an affidavit is not necessary. In such cases it will be sufficient to submit an LHM briefly setting forth the fact that a request for emergency electronic surveillance was made, the basis for such request, and the reason why such surveillance became unnecessary.

(7) It should be emphasized that the above-described procedures under which emergency Title III authorization can be obtained do not in any way eliminate the need to comply with the

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 46

requirements of a nonemergency Title III application since one may intercept communications under oral emergency authority only ". . . IF AN APPLICATION FOR AN ORDER APPROVING THE INTERCEPTION IS MADE IN ACCORDANCE WITH THIS SECTION WITHIN FORTY-EIGHT HOURS AFTER THE INTERCEPTION OCCURRED, OR BEGINS TO OCCUR . . ." (Emphasis added). The net effect of the emergency authorization process is that, following receipt of emergency authority, the entire nonemergency process must be undertaken, but within a much shorter period of time (48 hours).

(8) With regard to oral communication (microphone interceptions as opposed to wire interceptions), it is important to note that Title III authority is, by definition (see Title 18, USC, Section 2510 (2)), required when such oral communications are uttered by a person who exhibits a justifiable expectation of privacy. In the absence of such justifiable expectation (e.g., a forcibly occupied building, the residence of a stranger or of a hostage, and similar situations), no Title III court order is necessary for interception of the communications. Prior approval for such interceptions must be obtained in the same manner required for the approval of consensual monitoring of nontelephonic oral communications. Nontelephonic consensual monitoring in criminal matters may be approved by the SAC, except when one or more of the seven sensitive circumstances listed in MIOG, Part II, 10-10.3 (1) is present. Requests for authority to conduct consensual monitoring when the seven sensitive circumstances are present can be approved by the SAC when an emergency situation exists, and must be submitted to FBIHQ for Department of Justice approval in routine situations. (See MIOG, Part II, 10-10.3(9).) A field office desiring to institute microphone surveillance in hostage or other emergency situations where the existence of a justifiable expectation of privacy is in doubt should telephone the request to CID, FBIHQ. (Where possible, such request should recite the opinion and recommendations of the field office Chief Division Counsel.) CID will furnish all known facts and recommendations to Office of the General Counsel (OGC), which will make the final determination regarding the presence or absence of a justifiable expectation of privacy. If OGC determines that there is no justifiable expectation of privacy in the particular situation, CID will orally authorize use of the microphone surveillance. The field office must follow with a teletype reciting the oral authorization given and the facts upon which the authorization was based. The subsequent confirming letter from CID to the DOJ should specifically include the AUSA's opinion, and should state the opinion of OGC with respect to the absence of a justifiable expectation of privacy and the basis for that conclusion. If OGC determines that a justifiable expectation of privacy does exist, Title III authority is, of course, necessary for the microphone

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 47

surveillance.

(9) With regard to microphone surveillance, it is noted that some electronic tracking devices (commonly referred to as "ETDs," "beepers," or homing devices) [REDACTED]

b2  
b7E

[REDACTED] have incidental microphone capabilities. Although the primary use of such devices may be for their homing capability, the incidental microphone capability of the devices may require that Title III court authorization be obtained prior to their use. SAC may authorize the use of such devices in criminal investigations. (See MIOG, Part II, 10-10.8.)

(10) Relative to the authority to make emergency entries to install microphones absent a court order. In a situation where there is determined to be a justifiable expectation of privacy, or installation would involve trespass, emergency Title III authority must first be obtained under Title 18, USC, Section 2518 (7). The U.S. Supreme Court held that the power of the courts to authorize covert entries ancillary to their responsibility to review and approve electronic surveillance applications is implicit in the Title III statute. OGC believes that authority for the investigative or law enforcement officer specially designated by the Attorney General (normally the Director) to approve entries to install microphones can logically be derived from the emergency provisions of the statute (Section 2518 (7)), and that this derivation of authority is consistent with the Court rationale. Since FBI policy requires the inclusion of a specific request for surreptitious entry authority in routine Title III affidavits when such entry is necessary, this request, along with the underlying basis, should, of course, appear in the affidavits submitted (within the 48-hour time frame) following emergency Title III authorizations.

EFFECTIVE: 02/28/97

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 48

10-9.11.1 Form 2 Report

(1) The Form 2 report, to be submitted by a field office upon completion of Title III ELSUR activity, is a form designed by the Administrative Office of the United States Courts (AOC), and is utilized by the Department of Justice (DOJ) and the AOC to obtain certain specific information relating to the administration of Title III physical activity, (i.e., actual monitoring, physical surveillance, etc., in direct support of the ELSUR) and the results obtained therefrom. Usually in April of each calendar year, the AOC publishes a booklet reporting all Title III activity for the previous calendar year. This report is required by Title 18, USC, Section 2519, of the Omnibus Crime Control and Safe Streets Act of 1968.

(2) FBIHQ, upon notification of the filing of an application for a Title III court order, will, on a case-by-case basis, forward by airtel under the substantive case caption of the field office involved, a prenumbered, precarboned Form 1 and Form 2 packet as provided to the FBI by the AOC. The Form 1 report consists of ply 1 and ply 2 of the packet. The Form 2 report consists of ply 3 and ply 4 of the packet.

(3) Form 2 reports and related correspondence are to be typewritten.

(4) On or before the 30th day following the denial of a Title III court order or the expiration of the authorized period of the order, including all extensions, the designated Special Agent will assist the prosecuting attorney in completing plies 1 and 2 (Form 1 portion of the packet) and items 1 through 6 of plies 3 and 4, (Form 2 portion of the packet) identical on both the Form 1 and Form 2. The Form 1 portion should remain with the prosecuting attorney. The prosecuting attorney shall then be responsible for providing the issuing judge the ply 1 and ply 2 (Form 1) for review, approval, and signature so that the court may forward the Form 1 to the AOC.

(5) Items 6 through 11 of plies 3 and 4 of the Form 2 report are to be completed by the designated Special Agent and not by the prosecuting attorney. Ply 3 of the Form 2 report is to be submitted to FBIHQ 60 calendar days following the termination of a court-authorized Title III. This rule will apply strictly to all Title IIIs, whether denied or granted, routine or emergency, except those authorized during the last 60-day period of the calendar year. Any Title III authorized during the last 60 days of the calendar year or terminating on or before December 31 are to be submitted to FBIHQ no later than five working days following termination of the Title

Sensitive

PRINTED: 02/18/98



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 49

III. This submission is to be made regardless of whether or not resource costs (Item 9B) of the installation, basically supplies and other items, are available at the time of submission. The ply 4 portion of the Form 2 is to be submitted appropriately to the prosecuting attorney.

(6) Any Title III expiring before midnight of December 31 should be reported to FBIHQ, telephonically, on the next working day following the termination of Title III activity. Thereafter, the Form 2 should be submitted to FBIHQ within five working days.

(7) In a joint or task force type investigation involving another agency, the agency which is responsible for recordkeeping procedures, as outlined in the MIOG, Part II, Section 10-9.9, shall be responsible for the preparation and submission of the Form 2 (plies 3 and 4 of the packet) in accordance with that agency's established procedures. It will be the responsibility of the designated Special Agent to maintain effective liaison with the responsible agency in order that all necessary statistics, costs, and results are compiled and reported on one Form 2 to be submitted by the responsible agency, if other than the FBI.

EFFECTIVE: 06/18/87

10-9.11.2 Completion of Form 2 Report

The following is a listing of each Section and Subsection set forth on the Form 2 report with an explanation of the information to be entered for each Section/Subsection.

(1) "COURT AUTHORIZING OR DENYING THE INTERCEPT"

The Form 2 shows the above caption as Item 1 and all ply copies of the Forms 1 and 2. The docket number is generally preprinted and is utilized to track the form itself. To properly complete item number one, the full name of the judge signing or denying the Title III court order should be shown, along with the identity of the court to include the exact street address and not a post office box number.

(2) "SOURCE OF APPLICATION"

(a) Subsection 2A "Official Making Application."

This section should be used to show the full name of the official

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 50

making the original application to the court, generally an Assistant United States Attorney. The title of the official making the original application should be shown with his or her telephone number and area code. The county and the agency name should be shown with the exact mailing address, not, Federal Building, with the name of a city and state.

(b) Subsection 2B "Prosecution Official Authorizing Application." The appropriate name to be shown is a DOJ official in Washington, D.C., not a United States Attorney or an Assistant. The word "same" may be shown only if a DOJ official was also the official making the original application, as shown in Subsection 2A.

(3) "OFFENSES (LIST MOST SERIOUS OFFENSE FIRST)"

Enter the offense(s) specified in the Title III order or application for an extension of the order (predicate offenses, i.e., ITSP, TFIS, etc., cited in application). List, in capital letters, and underline the most serious offense first, (only one offense should be underlined). The following controls should be used to determine the most serious offense:

(a) When two or more offenses are specified in the application, the offense with the highest maximum statutory sentence is to be classified as the most serious.

(b) When two of the offenses have the same maximum sentence, a crime against a person is to take priority over a crime against property.

When listing the offenses, a general description such as gambling, narcotics, racketeering, etc., will suffice. DO NOT cite the offense by title and section of the U.S. Code.

(4) "DURATION OF INTERCEPT"

Enter the number of days requested and the date of the application. Use the appropriate box to show whether the application was denied or granted and show the date of the order or denial of the order. If the application was granted with changes, changes should be listed in the column captioned "Granted With These Changes." That is to say, if the judge, the official making the application or the prosecuting attorney authorizing the application differs from those named in Item 1 and 2 above, the new individual should be named and identified by title in this section. Also, if emergency authorization was granted, it should be shown in this section along with the date

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 51

granted i.e., "Emergency Authority 9/1/86." Do not list source numbers or techniques authorized. If insufficient space exists in this section to show all changes, submit on plain bond paper with number of section and title, as an attachment to ply 3 of the Form 2.

(5) "TYPE OF INTERCEPT"

Check the appropriate block(s) and note the specific device if not telephone or microphone.

(6) "PLACE"

Check the appropriate block(s). Be specific as to the business type and other type location, if any.

NOTE: When this portion of the form has been completed, the Form 1 portion (plies 1 and 2) is to remain with the prosecuting attorney who shall then be responsible for providing the form to the issuing judge for review, approval and signature in order for the court to forward the Form 1 to the AOC. The authorizing judge is required to file the Form 1 report with the AOC within 30 days of the expiration of the order, including all extensions.

(7) "INSTALLATION"

Check the appropriate block; only one block should be checked.

(8) "DESCRIPTION OF INTERCEPTS"

Subsections 8A through 8F to be utilized to show:

(a) that date on which the last ELSUR installation was terminated;

(b) the specific number of days the installation was in actual use;

(c) the average frequency of intercepts per day, (rounded off to the nearest number). Divide the "Number of Communications Intercepted," (8E), by the "Number of Days in Actual Use," (8B), i.e., 131 intercepts divided by 29 days equals 4.51 or 5 intercepts per day.

(d) the number of identifiable individuals whose communications were intercepted, (count each person only one time even

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 52

if intercepted more often);

(e) the estimated number of communications intercepted, and

(f) the estimated number of incriminating communications intercepted.

(9) "COST"

(a) Subsection 9A "Nature and Quantity of Personnel Used to Install and Monitor." This section should be utilized to show the exact number of Special Agents (SAs) assigned to physically monitor, log, perform other administrative functions or work in any other capacity, specifically regarding the Title III itself. Also, the specific number of support (clerical) personnel utilized for tape transcription, duplication or other administrative support should be shown in this subsection. SA time should be shown in total number of work days, i.e., "65 Special Agents days." Use the same formulation for support personnel. If a joint operation, other agencies' (either state, local or Federal) personnel time should be shown by number of work days and broken down as above. If three Deputy Sheriffs were utilized for five days, show "15 Deputy Sheriff days." The expended personnel time of other Federal agencies should be listed in the same manner. Do not co-mingle state, local, or Federal time. "Personnel Cost" segment should be left blank. Cost figures will be computed at FBIHQ. Therefore, it is necessary that accurate and specific information be furnished to FBIHQ via this form.

(b) Subsection 9B "Nature of Other Resources (Cost of Installation, Supplies, etc.)." Requires specific cost figures which pertain to the Title III itself. For instance, leased line figures, if available at the time of reporting; equipment or tools necessary for the specific installation(s) and any other supplies, not to include tapes, unless purchased with case funds specifically for this case. This resource cost is to be shown in the block to the right of item 9B marked "Resource Cost." The "Total Cost" figure is to be left blank.

(10) "RESULTS"

This subsection should be executed when results have been obtained. Do not place the words "not applicable" or "N/A" in this subsection. This subsection should be utilized in much the same manner as an FD-515 (Accomplishment Report Form).

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 53

Items 10A through 10D are to be utilized to show:

(a) "Number of Persons Arrested" (or otherwise taken into Federal custody, i.e., pre- or post-indictment summons) & "Arrest Offenses." Enter the total number of persons arrested. Count each person only once regardless of the number of offenses charged. List all offenses charged in the arrests. Again, a general description such as gambling, narcotics, racketeering, etc., will suffice. (Do not enter individual's name and do not use U.S. Code citations.)

(b) "Number of Motions to Suppress." Enter the number of motions to suppress (quash evidence) which were granted, denied and are still pending.

(c) "Number of Persons Convicted" & "Conviction Offenses." Enter the total number of persons convicted as a result of the interception and the offenses, by general description, for which the convictions were obtained. Persons who pled guilty would be counted in this category. Again, count each convicted person only once. (Report upon conviction. Not necessary to await sentencing.)

(d) "Number of Trials Completed." Enter the number of trials resulting from this Title III installation which have been completed. Do not count as a trial any instance where a plea was taken during the trial. Also, do not count any grand jury information such as dismissal of indictment.

(11) "COMMENTS AND ASSESSMENT"

This subsection should be utilized mainly to show if two or more Title III installations are related. This may be shown by inserting the words "related to document number \_\_\_\_\_." All Form 2s are prenumbered, and the docket number for the related Form 2 should be shown. The remaining sections of item number 11 should be left blank. The prosecutor's signature and date of report are to be left blank. (These blocks are executed by the Attorney General or Attorney General's designee in Washington, D.C., at the time of the Annual Report.)

Retain one copy of the completed Form 2 (ply 3) in a field office control file and one copy in the 1A Section of the substantive case file for supplemental submissions and recordkeeping purposes.

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 54

EFFECTIVE: 06/18/87

10-9.11.3 Submissions of Form 2 Report to FBIHQ

(1) Appropriate administrative controls are to be utilized by field offices to ensure accurate and timely submission of the Form 2. The Special Agent to whom the case is assigned and his/her supervisor are administratively responsible for the Form 2 report. SACs are "responsible" for the accuracy of the content of all Form 2 reports and their timely submission.

(2) The report is to be forwarded by airtel in a plain brown envelope, sealed and clearly marked:

Director, FBI  
ELSUR Index  
FBIHQ

The airtel will include the following information:

(a) Complete case title and name of Special Agent executing Form 2.

(b) List of principals named in the initial application for the specific Title III. Should principals be added in an extension application, these names are to be listed and identified with the specific extension order, i.e., "1st extension," "2nd extension," etc.

(c) The annual salary of any non-FBI personnel listed in Item 9, Subsection 9A, used to install and/or monitor the Title III.

(d) Should a case be deemed sensitive to the point that any information disseminated outside the FBI or DOJ would compromise the investigation or witnesses, etc., a detailed statement must be made in the airtel relative to the reason why the Form 2 report should not be sent to DOJ for dissemination to the AOC for publication.

(e) The names required in Item "(b)" above are to be listed, in the format as described, on a white 3 X 5 inch card captioned "Principals," followed by the docket number (corresponding to the docket number on the Form 2), and the names of the individuals

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 55

named as principals in the initial application and each extension thereof. This 3 X 5 inch card is to accompany the airtel and Form 2 report submitted to FBIHQ.

EFFECTIVE: 06/18/87

10-9.11.4 Supplemental Form 2 Reports

(1) Supplemental reports pertaining to statistical information called for in Item 10, caption "RESULTS" are included in each calendar year Title III report made by the AOC. The results called for in the supplemental report pertain to Title III ELSUR activity conducted during prior calendar years. Therefore, supplemental reports are to be submitted to FBIHQ as indicated in 10-9.11.3, above and subsequent to the submission of the original Form 2. The supplemental reports are to be submitted to FBIHQ by no later than close of business November 15 of each individual calendar year. Field offices will be reminded of this required submission by annual airtel to all SACs.

(2) If no supplemental information has been developed, that is to say, no further statistical information exists for the case or is forthcoming pertaining to the Title III, field offices are to submit an airtel to FBIHQ setting forth the fact that no supplemental information will be submitted and giving reason, i.e., case closed, trial set for following year, etc.

(3) The November 15 deadline will be extended only in the event statistical information is to be routinely reported by Form 2 within the same calendar year the original Form 2 is submitted. This information could include arrests, convictions (not necessarily to include sentencing), number of trials completed or major seizures prior to the end of the calendar year. Further, if no additional statistics are expected to be reported, the field office should so state in the submitting airtel.

(4) The additional information to be reported should be added to the copies of the previously submitted ply 3 of the Form 2 retained in the 1A section of the substantive case file and the field office designated control file. The form should then be duplicated and forwarded to FBIHQ. A copy of supplemental Form 2 should be retained in the 1A section of the substantive case file and the field office designated control file.

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 56

(5) For further guidance regarding the execution of a Form 2, refer to the "ELSUR WORKING GUIDE," Title III Section, pages 68 and 68.01.

(6) Special Agents preparing Form 2 reports should note the Form 2s are to be prepared and submitted by Special Agents, not Assistant United States Attorneys or other DOJ officials, notwithstanding instructions appearing at the bottom of ply 3 of the Form 2.

EFFECTIVE: 06/18/87

10-9.12 ELSUR Indexing in Title III Criminal Matters

The ELSUR support employee in each field division will index or supervise the indexing and review of all ELSUR cards in Title III matters prior to their submission to FBIHQ. This is to ensure all cards are complete, accurate and in a format specified herein. (For indexing procedures, refer to the "Index Guide" available at each field office through the File Assistant/ELSUR support employee.) In Title III matters, all ELSUR cards will be typewritten. Two original cards will be prepared, one to be forwarded to FBIHQ for inclusion in the FBIHQ ELSUR Index and one to be maintained in the field office ELSUR index. If the information appearing on an ELSUR card is classifiable, the card must be classified in accordance with standard classifying procedures. For indexing purposes, microphone surveillance (MISUR) being utilized in conjunction with either a closed circuit television (CCTV) surveillance or an electronic tracking device will be treated as a microphone surveillance.

(1) Principal Cards - 3-x-5-inch cards maintained in the ELSUR indices containing the true name or best-known name of targets of Title III electronic surveillances. The term "principal" means any individual specifically named in the application furnished the court as being expected to be monitored during the course of the electronic surveillance. Included on the Principal card is the term "Principal Title III"; the control number assigned the source, the Bureau file number, if known; and the field office file number. In Title III matters, Principal cards are prepared on blue index cards and are to be submitted to FBIHQ within ten working days of the date the application is filed with the court regardless of whether or not authorization is granted and whether or not an installation is made or activated. In the event that a new individual(s) is named in an application for an extension or amendment of a court order, ensure

Sensitive  
PRINTED: 02/18/98



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 57

Principal cards are submitted on the new individual(s).

Example of Principal Card

Principal Title III (Blue 3-x-5-inch index card)

- |                        |
|------------------------|
| a. SMITH, JOHN         |
| b. PRINCIPAL TITLE III |
| c. AL NDNY-1           |
| d. 182-111             |
| e. AL 182-1            |

(2) Proprietary Interest Cards - 3-x-5-inch cards maintained in the ELSUR Index identifying the entity(s) and individual(s) who own, lease, license, or otherwise hold a possessory interest in locations subjected to electronic surveillance. These cards also identify the locations, telephone numbers, vehicle identification number, etc., targeted in the Title III application. Proprietary Interest cards further include the control number assigned the source; the date the surveillance was instituted; space for the date it will be discontinued; Bureau file number if known; and field office file number. Proprietary Interest cards should be prepared in a manner so as to be retrievable by the name of the proprietor(s), the location, and each facility specified in the application. Accordingly, to accomplish this cross-referencing, an appropriate number of these cards should be prepared, interchanging the top three entries in conformity with proper cross-indexing and filing procedures. In Title III matters Proprietary Interest cards are prepared on blue index cards. Where electronic surveillance devices are being installed on a motor vehicle, the vehicle identification number (and not the license number) will appear as item "c." All Proprietary Interest cards are to be submitted to FBIHQ within ten working days of the date the application is filed with the court, regardless of whether or not authorization is granted by the judge and whether or not an installation is made or activated. In the event that a new location or facility is identified in an application for an extension or amendment of a court order, ensure Proprietary Interest cards are submitted reflecting this new or modified information within

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 58

ten working days of the date the application is filed with the court.

(a) Examples of Proprietary Interest Cards for  
Telephone Surveillance (TESUR) Coverage in Title III Criminal Matters

1. Proprietary Interest card for filing by  
name(s).

- a. SMITH, JOHN
- b. 202-324-3300
- c. 901 Elm Avenue, Room 300  
Albany, New York  
Holiday Inn
- d. AL NDNY-1
- e. Instituted: 11-1-82
- f. Discontinued: (to be filled in later)
- g. 182-000
- h. AL 182-12

2. Proprietary Interest card for filing by  
telephone number.

- b. 202-324-3300
- a. SMITH, JOHN
- c. 901 Elm Avenue, Room 300  
Albany, New York  
Holiday Inn
- d. AL NDNY-1
- e. Instituted: 11-1-82
- f. Discontinued: (to be filled in later)
- g. 182-1000
- h. AL 182-12

3. Proprietary Interest card for filing by  
address.

- c. 901 Elm Avenue, Room 300  
Albany, New York  
Holiday Inn
- a. SMITH, JOHN

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 59

- b. 202-324-3300
- d. AL NDNY-1
- e. Instituted: 11-1-82
- f. Discontinued: (to be filled in later)
- g. 182-1000
- h. AL 182-12

4. Proprietary Interest card for filing by facility.

- c. Holiday Inn  
901 Elm Avenue, Room 300  
Albany, New York
- a. SMITH, JOHN
- b. 202-324-3300
- d. AL NDNY-1
- e. Instituted: 11-1-82
- f. Discontinued: (to be filled in later)
- g. 182-1000
- h. AL 182-12

(b) Examples of Proprietary Interest Cards for TESUR Coverage in Title III Criminal Matters Wherein More Than One Person Owns, Leases, Licenses, or Otherwise Holds a Possessory Interest in the Property Subjected to the Surveillance

1. Proprietary Interest card for filing by name(s).

- a. SMITH, JOHN  
JONES, SARA
- b. 202-324-3300
- c. 901 Elm Avenue  
Albany, New York  
ABC Trucking Co.
- d. AL NDNY-1
- e. Instituted: 11-1-82
- f. Discontinued: (to be filled in later)
- g. 182-1000
- h. AL 182-12

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 60

2. The above card will be filed under the name of SMITH, JOHN and another should be prepared for filing under the name of JONES, SARA.

- a. JONES, SARA  
SMITH, JOHN
- b. 202-324-3300
- c. 901 Elm Avenue  
Albany, New York  
ABC Trucking Co.
- d. AL NDNY-1
- e. Instituted: 11-1-82
- f. Discontinued: (to be filled in later)
- g. 182-1000
- h. AL 182-12

3. Proprietary Interest card for filing by telephone number.

- b. 202-324-3300
- a. SMITH, JOHN  
JONES, SARA
- c. 901 Elm Avenue  
Albany, New York  
ABC Trucking Co.
- d. AL NDNY-1
- e. Instituted: 11-1-82
- f. Discontinued: (to be filled in later)
- g. 182-1000
- h. 182-12

4. Proprietary Interest card for filing by address.

- c. 901 Elm Avenue  
Albany, New York  
ABC Trucking Co.

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 61

- a. SMITH, JOHN  
JONES, SARA
- b. 202-324-3300
- d. AL NDNY-1
- e. Instituted: 11-1-82
- f. Discontinued: (to be filled in later)
- g. 182-1000
- h. AL 182-12

5. ~~Proprietary Interest card for filing by~~  
facility.

- c. ABC Trucking Co.  
901 Elm Avenue  
Albany, New York
- a. SMITH, JOHN  
JONES, SARA
- b. 202-324-3300
- d. AL NDNY-1
- e. Instituted: 11-1-82
- f. Discontinued: (to be filled in later)
- g. 182-1000
- h. AL 182-12

(c) Example of Proprietary Interest Card for MISUR  
Coverage in Title III Criminal Matters

1. Proprietary Interest card for filing by  
name.

- a. SMITH, JOHN
- b. MISUR
- c. 901 Elm Avenue, Room 300  
Albany, New York  
Holiday Inn
- d. AL NDNY-2
- e. Instituted: 11-1-82
- f. Discontinued: (to be filled in later)
- g. 182-1000
- h. AL 182-12

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 62

address

2. Proprietary Interest card for filing by the

c. 901 Elm Avenue, Room 300 Albany, New York Holiday Inn
a. SMITH, JOHN
b. MISUR
d. AL NDNY-2
e. Instituted: 11-1-82
f. Discontinued: (to be filled in later)
g. 182-1000
h. AL 182-12

facility.

3. Proprietary Interest Card for filing by

c. Holiday Inn 901 Elm Avenue, Room 300 Albany, New York
a. SMITH, JOHN
b. MISUR
d. AL NDNY-2
e. Instituted: 11-1-82
f. Discontinued: (to be filled in later)
g. 182-1000
h. AL 182-12

(d) Example of Proprietary Interest Card for MISUR  
Coverage Involving a Vehicle in Title III Criminal Matters

name.

1. Proprietary Interest card for filing by

a. SMITH, JOHN
b. MISUR
c. VIN 1A2345RA789
d. AL NDNY-3
e. Instituted: 11-1-82
f. Discontinued: (to be filled in later)
g. 182-1000
h. AL 182-12

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 63

2. Proprietary Interest card for filing by the  
vehicle identification number.

- c. VIN 1A2345RA789
- a. SMITH, JOHN
- b. MISUR
- d. AL NDNY-3
- e. Instituted: 11-1-82
- f. Discontinued: (to be filled in later)
- g. 182-1000
- h. AL 182-12

No card for filing under the address is required in matters involving  
a motor vehicle.

(e) Example of Proprietary Interest Cards for CCTV  
Coverage in Connection With MISUR Coverage

1. Proprietary Interest card for filing by  
name.

- a. SMITH, JOHN
- b. MISUR
- c. 901 Elm Avenue, Room 300  
Albany, New York  
Holiday Inn
- d. AL NDNY-3
- e. Instituted: 11-1-82
- f. Discontinued: (to be filled in later)
- g. 182-1000
- h. AL 182-12

2. Proprietary Interest card for filing by the  
address.

- c. 901 Elm Avenue, Room 300  
Albany, New York  
Holiday Inn
- a. SMITH, JOHN
- b. MISUR
- d. AL NDNY-3

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 64

- e. Instituted: 11-1-82
- f. Discontinued: (to be filled in later)
- g. 182-1000
- h. 182-12

3. Proprietary Interest card for filing by the facility.

- c. Holiday Inn  
901 East Avenue, Room 300  
Albany, New York
- a. SMITH, JOHN
- b. MISUR
- d. AL NDNY-3
- e. Instituted: 11-1-82
- f. Discontinued: (to be filled in later)
- g. 182-1000
- h. 182-12

In most situations when Proprietary Interest cards are prepared, item "f" will not be known. In some situations, items "d" and "e" may not be known. When this information is determined, it should be furnished to FBIHQ, by airtel, or an amended card(s) should be prepared.

(3) Overhear Cards - 3-x-5-inch cards maintained in the ELSUR indices containing the true name or best-known name of all individuals (including non-U.S. persons, Special Agents, assets, informants, cooperating witnesses, etc.) who have participated in conversations intercepted during the conduct of a Title III electronic surveillance. Only one Overhear card is required per source for any individual overheard, regardless of the number of times his/her voice is overheard. If the individual is overheard on more than one source, a separate Overhear card should be submitted to FBIHQ for each source the first time an individual is overheard. As the ELSUR indices maintained at FBIHQ will only contain one Overhear card the first time an individual is overheard on a specific source, it will be the responsibility of the field office to maintain records of all subsequent overhears of that individual over the same source. Accordingly, the field office should enter the date of each subsequent overhear on the card maintained on that individual in the field office ELSUR indices. Overhear cards are only submitted if the identity of the individual overheard is known or a full name is given. In the event that a partial name, code name, nickname or alias overheard

Sensitive

PRINTED: 02/18/98



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 65

during an electronic surveillance is positively identified with a specific individual through investigation or further monitoring, an Overhear card is then submitted to FBIHQ. The overhear date will be the earliest date the individual was monitored over that source and all subsequent overhears determined to be identical to that individual should be recorded on the field office ELSUR card. In addition to the name of the individual overheard, Overhear cards contain the date on which the conversation took place; the symbol number assigned to the source; Bureau file number, if known; and the field office file number. In Title III matters, Overhear cards are prepared on blue index cards and submitted to FBIHQ within a reasonable period of time, not to exceed 30 calendar days following the first instance an individual is identified as having been overheard over each different ELSUR installation. All Overhear cards will be submitted to FBIHQ, in accordance with instructions for the submission of ELSUR cards.

Example of Overhear Card in Title III Matters

Overhear Title III, TESUR or MISUR coverage.

- a. SMITH, JOHN
- b. 12-7-81
- c. AL NDNY-1
- d. 182-111
- e. AL 182-1

Any additional information a field office deems necessary for inclusion on any type ELSUR card being forwarded to FBIHQ should be labeled on the card and explained in a brief statement in the FD-664. As an example, an auxiliary office submitting Overhear cards to FBIHQ as the result of an ELSUR conducted at the request of another field office may wish to reflect on the Overhear card the file number of the office of origin. An Overhear card prepared in this manner would appear as follows:

- a. SMITH, JOHN
- b. 12-7-81
- c. AL NDNY-1
- d. 182-11
- e. AL 182-11
- f. OO: BS 182-12

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 66

It would not be necessary for the auxiliary office to prepare copies of the Overhear cards for inclusion in the ELSUR index of the office of origin; to forward a copy of the FD-664 to the office of origin for information purposes is sufficient.

EFFECTIVE: 06/06/86

10-9.13 Marking of Recordings for Identification

See Part II, 16-8.2.3 of this manual.

EFFECTIVE: 09/22/87

10-9.14 Loan of Electronic Surveillance Equipment to State and  
Local Law Enforcement Agencies

See Part II, |16-7.3.4| of this manual.

EFFECTIVE: 09/22/87

10-9.15 Submission of Recordings

For instructions regarding the forwarding of tapes to  
FBIHQ see Part II, 16-8.2.4 and 16-8.2.8 of this manual, and MAOP,  
| Part II, |2-4.4.11. |

EFFECTIVE: 10/16/96

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 67

10-9.16 Transcription of Recordings

(1) FD-652, Transcription Request/Approval Sheet, should accompany each request for transcription of any tape. Include on the FD-652, under "Summary," information describing where the discussion/meeting took place, what the subject of the conversation was, and any other details that would be helpful to the typist in accurately transcribing tape recordings. It is mandatory that the SAC grant approval for all full-text transcriptions and indicate this approval by initialing the appropriate block on FD-652. The final disposition of this form is being left to the discretion of each individual office. They may be disposed of in the same manner as the FD-77 (Dictation Slip). (See MAOP, Part II, Section 10-18.1(4), for use of FD-77.)

(2) For additional instructions regarding the preparation of transcripts of recordings, see Correspondence Guide - Field, Section 2-11.6.

EFFECTIVE: 04/19/91

10-10 CONSENSUAL MONITORING - CRIMINAL MATTERS

EFFECTIVE: 04/19/91

10-10.1 Use of Consensual Monitoring in Criminal Matters

(1) Consensual monitoring is the interception by an electronic device of any wire or oral communication wherein one of the parties to the communication has given prior consent to such monitoring and/or recording.

(2) Title 18, USC, Section 2511 (2)(C), requires consent from one of the parties to the communication to bring the interception within an exception to the general warrant requirement. To document conformance to the requirements of the statute, FBI policy requires that a consent form be obtained from the consenting party. (See MIOG, Part II, 10-10.3(7).)

(3) No exception should be made to executing and properly witnessing the consent form in the situation wherein an informant, cooperative witness (CW), a Special Agent or any other law enforcement

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 68

officer is the consenting party. Additionally, the consent form constitutes an accurate, reliable official record that may be utilized in a court in the event the issue of consent is raised or the administrative procedure needs to be documented to assure the court compliance with Title 18, USC, Section 2511 (2)(C). (See MIOG, Part II, 10-10.3(7).)

(4) Separate control files -- One for telephonic consensual monitoring and another for nontelephonic consensual monitoring (body recorders and/or transmitting devices) should be established in each field office. Documents relative to the authorization and utilization of these techniques should be retained in the appropriate control file. These control files will be for the purpose of the SAC's administrative control and for use during the inspection.

(5) In matters involving the use of Closed Circuit Television (CCTV) in conjunction with the consensual monitoring technique, refer also to Part II, 10-9.10(7) and 10-10.9 of this manual.

EFFECTIVE: 02/28/97

10-10.2 Monitoring Telephone Conversations in Criminal Matters  
(See MIOG, Part I, 89-2.11(7), 91-11.3.2(2), 192-14(2);  
Part II, 10-9.9(3), 16-7.4.1.)

An FD-670, Checklist - Consensual Monitoring - Telephone (Criminal Matters) form, lists all recordkeeping and operational requirements specified in the MIOG, MAOP, and the "ELSUR Working Guide." This form is available for optional use as a reference and training aid to ensure adherence to all existing Bureau requirements.

(1) SACs may authorize monitoring of telephone conversations in criminal matters for the duration of the investigation. Each authorization should be documented on Form FD-759 (Notification of SAC Authority Granted for Use of CONSENSUAL Monitoring Equipment), and may be granted under the conditions that:

(a) Agents should obtain written consent (for all ELSURs not approved by an appropriate court), as documented by an executed Form FD-472 (Telephone Device Consent), whenever possible; however, oral consent will be acceptable in those instances where the

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 69

consenting party declines to give written consent. When oral consent is obtained, at least two Law Enforcement Officers (one of whom should be an Agent of the FBI) should be present to witness this consent. The fact that the consenting party has declined to give written consent should be recorded on the FD-472. This form should then be executed in all respects with the exception of the consenting party's signature. Once the consent form has been obtained, it will not be necessary to obtain a separate consent form for each instance wherein conversations are to be monitored and/or recorded. It is sufficient if the consent form is signed for each investigation so long as the office has obtained telephonic consensual monitoring authority and the subject matter for which the authority was granted; the consenting party or parties to the interception; and/or the judicial district do not change. This consent form shall remain valid until such time as the consenting party expresses the desire, either orally or in writing, to a Special Agent of the FBI to rescind the consent;

(b) Prior to its initial use, the USA, AUSA, or Strike Force Attorney for the particular investigation in which the monitoring will be utilized should provide an opinion that no entrapment is foreseen and concur with the monitoring and/or recording of the conversation as an investigative technique. This initial concurrence should be confirmed in writing. Whenever a change in parties or circumstances occur, subsequent opinions should be obtained and confirmed in writing. (See MIOG, Part II, 10-10.3 (12).)

(c) Consensual monitoring conducted outside the division in which authorization is obtained requires coordination with and concurrence from the SAC of each division where the monitoring will occur. Such concurrence must be documented in writing by the office of origin if not documented by the lead office in the EC forwarding the recordings to the requesting office.

(d) A separate control file for telephone monitoring should be established in each field office and appropriate documents relative to the authorization and utilization of this procedure should be retained. This control file will be for the purpose of the SAC's administrative control and for review during inspection.

(e) The FD-759 is to be typewritten, completed in its entirety and forwarded as indicated on the copy count of the form within ten working days of the date authority is granted as indicated in Item 5 of the form. In those investigations wherein both telephonic and nontelephonic consensual monitoring authority is granted, SAC approval may be documented on one FD-759. This may be done only when both techniques are being used in the same

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 70

investigative case and all facts required on the FD-759 are the same for both techniques. Any variations in the facts contained on the FD-759 will require two separate FD-759s, such as more than one consenting party or the duration for which the authority is granted for each technique differs, etc. Telephonic consensual monitoring authority is case specific and is not transferrable to any other investigation except when the case file under which the authority was granted is consolidated or reclassified. FD-759s documenting only telephonic consensual monitoring authority need not be forwarded to FBIHQ. (See MIOG, Part II, 10-10.3 (1).)

(2) In cases of extreme sensitivity, SACs should continue to obtain FBIHQ authority for consensual monitoring of telephone conversations. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 specifically exempts consensual monitoring (both telephonic and body recording equipment) from the provisions of the statute.

(3) In certain situations, it may be more effective and efficient to utilize three-way or conference calling in conjunction with approved telephonic consensual monitoring. Once consent forms have been signed and authorization received, three-way or conference calling may be used to make more efficient use of an Agent's time and/or to alleviate the necessity for face-to-face contact with the consenting party, thereby avoiding the compromise of a covert investigation. However, the use of conference calling is not appropriate in all cases. In some instances, it may be desirable for the Agent to be with the consenting party at the time the call is placed in order that the Agent may utilize notes or gestures to provide information and guidance to the consenting party during the course of the call.

EFFECTIVE: 09/17/97

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 71

[REDACTED]

XXXXXX  
XXXXXX  
XXXXXX

FEDERAL BUREAU OF INVESTIGATION  
FOIPA  
DELETED PAGE INFORMATION SHEET

Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

- Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552

Section 552a

(b)(1)

(b)(7)(A)

(d)(5)

(b)(2)

(b)(7)(B)

(j)(2)

(b)(3)

(b)(7)(C)

(k)(1)

(b)(7)(D)

(k)(2)

(b)(7)(E)

(k)(3)

(b)(7)(F)

(k)(4)

(b)(4)

(b)(8)

(k)(5)

(b)(5)

(b)(9)

(k)(6)

(b)(6)

(k)(7)

- Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

- Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

Pages were not considered for release as they are duplicative of \_\_\_\_\_

Page(s) withheld for the following reason(s): \_\_\_\_\_

- The following number is to be used for reference regarding these pages: \_\_\_\_\_

XXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X for this page X  
XXXXXXXXXXXXXXXXXXXXX

XXXXXX  
XXXXXX  
XXXXXX



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 73

[REDACTED]

[REDACTED]

[REDACTED]

EFFECTIVE: 05/10/96

10-10.3 Monitoring Nontelephone Communications In Criminal Matters  
(See MIOG, Part I, 7-14.6(14), 9-7.2(5), 91-11.3.3,  
192-15; Part II, 10-9.9(3), 10-10.9.3(1), 16-7.4.1; &  
Legal Handbook for Special Agents, 8-3.3.3(1).)

An FD-671, Checklist - Consensual Monitoring -  
Nontelephone (Criminal Matters) form, lists all recordkeeping and  
operational requirements specified in the MIOG, MAOP, and the "ELSUR  
Working Guide." This form is available for optional use as a  
reference and training aid to ensure adherence to all existing Bureau  
requirements.

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 74

(1) Nontelephonic Consensual Monitoring (NTCM) in criminal matters may be approved by the SAC, except when one or more of the seven sensitive circumstances is present. Requests for authority to conduct consensual monitoring when any of the seven sensitive circumstances are present will be submitted to FBIHQ for Department of Justice approval in ROUTINE situations, and can be approved by the SAC when an emergency situation exists. EMERGENCY situations are those wherein the monitoring is expected to take place within 48 hours. Emergency authority cannot exceed 30 days and requests for extension will be submitted to FBIHQ for Department of Justice approval. (See (3), (9) and (10).)

SAC approval for routine nonsensitive NTCM usage or for emergency NTCM usage involving sensitive circumstances is to be documented on Form FD-759 (Notification of SAC Authority Granted for Use of CONSENSUAL Monitoring Equipment). The FD-759 is to be typewritten, completed in its entirety and forwarded to the appropriate FBIHQ entities within ten working days of the date authority is granted as indicated in Item 5 of the form. (See MIOG, Part II, 10-10.2 (1) (e).) NTCM authority is case specific and is not transferrable to any other investigation except when the case file under which the authority was granted is consolidated or reclassified.

SAC authority to approve NTCM usage in all but the seven sensitive circumstances may not be redelegated; however, an acting SAC may authorize Agents to conduct routine consensual monitoring, if specifically and individually designated by the SAC to act in his/her stead when the SAC is absent. (See MIOG, Part II, 10-9.11 (8).) The seven sensitive circumstances are as follows:

(a) The interception 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;

(b) The interception relates to an investigation of any public official and the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his or her official duties. (Public official is defined as an official of any public entity of government including special districts as well as all federal, state, county, and municipal governmental units.);

(c) The interception relates to an investigation of

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 75

a federal law enforcement official;

(d) The consenting or nonconsenting person is a member of the diplomatic corps of a foreign country;

(e) The consenting or nonconsenting person is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers;

(f) The consenting or nonconsenting person is in the custody of the Bureau of Prisons or the United States Marshals Service; in cases where the individual is in the custody of the Bureau of Prisons or the United States Marshals Service, the field office teletype requesting authorization for use of consensual monitoring devices on a prisoner, or a request for a furlough or extraordinary transfer of a prisoner, must contain the following information in addition to that information set out in 10-10.3 (9):

1. The location of the prisoner;
2. Identifying data concerning the prisoner (FBI number, inmate identification number, social security number, etc.);
3. The necessity for using the prisoner in the investigation;
4. The name(s) of the target(s) of the investigation;
5. Nature of the activity requested (wear consensual monitoring device, furlough, extraordinary transfer);
6. Security measures to be taken to ensure the prisoner's safety if necessary;
7. Length of time the prisoner will be needed in the activity;
8. Whether the prisoner will be needed as a witness;
9. Whether a prison redesignation (relocation) will be necessary upon completion of the activity;
10. Whether the prisoner will remain in the

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 76

custody of the FBI or whether he/she will be unguarded except for security purposes.

The authority of the SAC to approve consensual monitoring when an emergency situation exists does NOT alter the requirement for prior DOJ authorization to use a prisoner who is in the custody of the Bureau of Prisons (BOP), or the United States Marshals Service (USMS). Accordingly, field offices are required to continue coordinating the use of a prisoner, who is the subject of consenting or nonconsenting monitoring, through FBIHQ as set forth in MIOG, Part II, 10-10.3 and 27-16.5.

(g) ~~The Attorney General, Deputy Attorney General, Associate Attorney General, Assistant Attorney General for the Criminal Division, or the United States Attorney in a district where an investigation is being conducted has requested the investigating agency to obtain prior written consent for making a consensual interception in a specific investigation.~~

The presence of one or more of the above seven circumstances requires Office of Enforcement Operations, DOJ approval. Additionally, all requests requiring DOJ approval shall be reviewed and approved by the Chief Division Counsel (CDC) prior to submission of the communication to FBIHQ with the name of the CDC stated in the requesting communication.

(2) The Guidelines also mandate the FBI's obtaining prior authorization from the United States Attorney, Assistant United States Attorney, Strike Force Attorney or any other previously designated DOJ attorney for the particular investigation in which the monitoring will be utilized.

(3) The Director has delegated authority to the SAC to approve NTCM of verbal communications except when the circumstances listed in MIOG, Part II, 10-10.3 (1) above, are present. SACs 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 to determine whether or not the NTCM authority should continue or new authority obtained. Where new authority is obtained, a new FD-759 must be completed.

(4) Consensual monitoring conducted outside the division

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 77

in which authorization was obtained requires coordination with and concurrence from the SAC of each division where the monitoring will occur. Such concurrence must be documented in writing by the office of origin if not documented by the lead office in the EC forwarding the recordings to the requesting office.

(5) Agents should obtain written consent, documented by an executed FD-473 (Nontelephone Device Consent) form, whenever possible. However, oral consent will be acceptable in those instances where the consenting party declines to give written consent. When oral consent is obtained, at least two Law Enforcement Officers (one of whom should be an Agent of the FBI) should be present to witness this consent. The fact that the consenting party has declined to give written consent should be recorded on the FD-473. This form should then be executed in all respects, with the exception of the consenting party's signature.

(6) Once the consent form has been obtained, it will not be necessary to obtain a separate consent form for each instance wherein communications are to be monitored and/or recorded. It is sufficient if the consent form is signed for each investigation so long as the office is continuing to operate under the same authority and the subjects (target(s) and consenting party) do not change. This consent form shall remain valid until such time as the consenting party expresses the desire, either orally or in writing, to a Special Agent of the FBI to rescind the consent.

(7) No exception should be made to executing and properly witnessing the consent form in the situation wherein an informant, cooperative witness (CW), a Special Agent or any other law enforcement officer is the consenting party. (See MIOG, Part II, 10-10.1 (2) and (3).) The consent form constitutes an accurate, reliable, official record that may be utilized in a court in the event the issue of consent is raised or the administrative procedure needs to be documented to assure the court compliance with Title 18, USC, Section 2511 (2) (c). As in any case involving consensual monitoring, it is essential that the consenting party be present at all times when the monitoring equipment is activated.

(8) SAC or DOJ authority is required in joint operations with nonfederal law enforcement agencies in which FBI nontelephone monitoring equipment will be used. (See MIOG, Part II, 16-7.3.4(2).)

(9) In requesting Department of Justice (DOJ) authority for use of nontelephonic consensual monitoring equipment in routine situations when any of the seven sensitive circumstances listed in

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 78

MIOG, Part II, 10-10.3 (1) exists, it will be necessary to use the following format in the field communication. Only in the Administrative Data portion of this communication should the consenting party be identified (if protection is sought) by symbol number or name. This communication may be furnished directly to the Department: (See MIOG, Part II, 10-9.11(8) & 10-10.3(1)(f), above.)

**PURPOSE:** Authority is requested to utilize an electronic device to monitor and/or record private communications between \_\_\_\_\_ and \_\_\_\_\_ (if appropriate, insert "and others as yet unknown") in connection with a \_\_\_\_\_ (character) matter.

**DETAILS:** Begin with a sentence which states that this request requires DOJ approval and identify which of the seven sets of circumstances require such approval. Provide a statement that the Chief Division Counsel, identified by name, has reviewed and approved the communication for legal sufficiency. Describe background of case--reasons why the device is needed and when and where it is needed. Identify the person who is to wear the device or indicate if fixed device is to be used (body recorder, transmitter, Closed Circuit Television (CCTV), other) and where it will be installed (automobile, office, home of consenting party, etc.) and indicate it will only be used when consenting party is present. If a CW or an informant is the person whose identity should be protected, or if an Undercover Agent (UCA) is the consenting party, identify the person as "source." Show, under Administrative Data, the symbol number of the CW or informant, identity of UCA, or name of person whose identity is to be protected. Show, under Administrative Data, the type of device to be used and specifically state that consenting party is willing to testify in court and will execute the FD-473, or will give oral consent which will be witnessed by two law enforcement officers, one of whom should be an Agent of the FBI.

**U.S. ATTORNEY'S OPINION:** Identify USA, AUSA, or Strike Force Attorney with whom case discussed. Specifically set out USA's opinion regarding entrapment and specifically state USA approves the use of device.

**ADMINISTRATIVE DATA:** All administrative data should be shown in this section. Here only should the person who is to wear the device be identified (if protection is sought) by name or symbol number or indicate if fixed device.

(10) Where an emergency situation exists involving a sensitive circumstance, prior DOJ authorization is not required. Under such circumstances, the SAC may approve the request; however,

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 79

subsequent DOJ notification is required within five work days and will be handled by FBIHQ upon receipt of the Form FD-759. Emergency authority cannot exceed 30 days and requests for extension will be submitted to FBIHQ for Department of Justice approval. (See (1).)

(11) All offices should ENSURE appropriate administrative controls are established to ensure FBIHQ is advised of the results of the usage of consensual monitoring equipment within 30 days of the expiration of each SAC and/or DOJ authorization. If it is anticipated that an extension of DOJ authority will be needed, ensure that the requesting teletype is received at FBIHQ at least seven days prior to the expiration of authority. Within 30 days of the expiration of each SAC or DOJ authorization and each extension thereof, an FD-621 (NTCM Usage Report), shall be prepared under the substantive case caption including the character of the case, completed in its entirety and forwarded to FBIHQ in an envelope sealed and labeled "Director, FBI, ELSUR Index, FBIHQ."

(12) The initial opinion of the USA, AUSA, or Strike Force Attorney regarding entrapment and concurrence in the use of the technique should be confirmed in writing. Whenever a change in parties or circumstances occurs subsequent opinions should be obtained and confirmed in writing. (See MIOG, Part II, 10-10.2(1)(b).)

EFFECTIVE: 09/17/97

10-10.4 Deleted

EFFECTIVE: 12/16/88

10-10.5 ELSUR Indexing in Consensual Monitoring Matters

The ELSUR support employee in each field division will index, or supervise the indexing of, and review all ELSUR cards in consensual monitoring matters, prior to their submission to FBIHQ. This is to ensure that all cards are complete, accurate and in a format specified herein. (For indexing procedures refer to the "Index Guide" available at each field office through the File Assistant/ELSUR support employee.) In consensual monitoring matters all ELSUR overhear cards will be typewritten. Two original cards will be prepared; one to be forwarded to FBIHQ for inclusion in the FBIHQ

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 80

ELSUR Index, and one to be maintained in the field office ELSUR index. If the information appearing on an ELSUR card is classifiable, the card must be classified in accordance with standard classifying procedures.

(1) Overhear Cards - 3-x-5 cards maintained in the ELSUR indices containing the true name or best-known name of all individuals (including non-U.S. persons, Special Agents, assets, informants, cooperating witnesses, etc.) who have participated in conversations intercepted during the conduct of a consensual monitoring matter. Only one Overhear card is required per source for any individual overheard, regardless of the number of times his/her voice is overheard. If the individual is overheard on more than one source, a separate Overhear card should be submitted to FBIHQ for each source the first time an individual is overheard. As the ELSUR indices maintained at FBIHQ will only contain one Overhear card the first time an individual is overheard on a specific source, it will be the responsibility of the field office to maintain records of all subsequent overhears of that individual over the same source. Accordingly, the field office should enter the date of subsequent overhears on the card maintained on the individual in the field office ELSUR indices. Overhear cards are only submitted if the identity of the individual overheard is known or a full name is given. In the event that a partial name, code name, nickname or alias overheard during an electronic surveillance is positively identified with a specific individual through investigation or further monitoring, an Overhear card is then submitted to FBIHQ. The overhear date will be the earliest date the individual was monitored over that source, and all subsequent overhears determined to be identical to that individual should be recorded on the field office ELSUR card. In addition to the name of the individual overheard, Overhear cards contain the date on which the conversation took place; the control number assigned to the source or the word "Consensual"; the technique ("telephone" or "nontelephone" spelled out); Bureau file number, if known; and the field office file number. In consensual monitoring matters, Overhear cards are prepared on white index cards. All Overhear cards will be submitted to FBIHQ, in accordance with instructions for the submission of ELSUR cards, within a reasonable period of time, not to exceed 30 calendar days following the first instance an individual is identified as having been overheard over each different ELSUR installation.

Examples of Overhear Card in Consensual Monitoring  
Matters

(a) Overhear Consensual Monitoring - Telephone

---

Sensitive  
PRINTED: 02/18/98



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 81

- a. SMITH, JOHN
- b. 12-7-82
- c. AL CM# 10 (Telephone) or Consensual (Telephone)
- d. 182-111
- e. AL 182-1

(b) Overhear Consensual Monitoring - Nontelephone

- a. SMITH, JOHN
- b. 12-7-82
- c. AL CM# 11 (Nontelephone) or Consensual  
Nontelephone)
- d. 182-111
- e. AL 182-1

(2) Any additional information a field office deems necessary for inclusion on any type ELSUR card being forwarded to FBIHQ should be labeled on the card and explained in a brief statement in the FD-664. As an example, an auxiliary office submitting Overhear cards to FBIHQ as the result of an ELSUR conducted at the request of another field office may wish to reflect on the Overhear card the file number of the office of origin. An Overhear card prepared in this manner would appear as follows:

- a. SMITH, JOHN
- b. 12-7-82
- c. AL CM # 12 (Nontelephone) or Consensual  
(Nontelephone)
- d. 182-111
- e. AL 182-11
- f. OO: BS 182-12

It would not be necessary for the auxiliary office to prepare copies of the Overhear cards for inclusion in the ELSUR index of the office of origin; to forward a copy of the FD-664 to the office of origin for information purposes is sufficient.

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 82

EFFECTIVE: 12/16/88

10-10.5.1 Administration of ELSUR Records Regarding Informants and Assets

(1) Title 18, USC, Section 3504, allows a claim to be made for disclosure of ELSUR information "...in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, or other authority of the United States...." Discovery motions may be made by a defendant in the proceedings, or on behalf of witnesses, and attorneys providing representation. However, in a motion for disclosure of ELSUR information involving a source who participated in consensual monitoring, a response by the government does not necessarily disclose the identity of the source (consenting party) and/or the confidential nature of the relationship that individual had with the FBI except in situations where a determination is made by the appropriate authority that source disclosure is relevant to the proceedings.

Every effort will be made by FBIHQ through liaison with the Department of Justice to prevent disclosure.

(2) To prevent unwarranted disclosures, the following procedures are to be used when a source is party to a consensual monitoring:

(a) Communications to FBIHQ requesting consensual monitoring authorization are to identify informants or assets by symbol number or other appropriate terminology.

(b) In the execution of the required consent form (FD-472, FD-473), the true name of the consenting party is to be used. When the consenting party is a source, the original of the executed form is to be retained in the evidence section of the source's main file.

(c) On the FD-504 (Chain of Custody-Original Tape Recording) envelope, the true name of the source is to be set forth in the space provided for the entry, "Identity of Persons Intercepted." The completed FD-504 is to be maintained in a limited or restricted access location in full compliance with the instructions set forth in Part II, Section 10-9.8, of this manual.

(d) Neither the true name nor the informant symbol

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 83

number is to be set forth on the FD-192 (Control of General/Drug/Valuable Evidence) form.

(e) FD-302s, transcripts, etc., pertaining to consensual monitorings are to be prepared and maintained in compliance with the instructions set forth in Part I, Section 137-10 of this manual; Section 2-11.6 through 2-11.6.4 of the Correspondence Guide-Field or in the Introduction, Section 1, of the Foreign Counterintelligence Manual. Because of the nature of consensual monitoring, particularly when a limited number of conversants are involved, strict adherence to these guidelines is essential to protect the identity of the source.

(f) Overhear cards are to be prepared for all reasonably identified participants to a consensually monitored conversation, including the consenting party. For sources, both the FBIHQ and the field office cards are to be prepared for the true name(s) of the individual(s) monitored. Except for required classification markings, as applicable, no additional notations are to be set forth on the cards submitted to FBIHQ to indicate the monitored person is a source or to indicate that there is any unique sensitivity to the consensual monitoring conducted. Such caveats may, however, be placed on the field office ELSUR cards, but must be documented to a specific serial which reflects the need for and duration of special handling.

(g) The airtel to FBIHQ (FD-664) enclosing ELSUR cards for sources is to be prepared and submitted as outlined in Section 10-9.5 above. The names being indexed by each card enclosed will be listed on the FBIHQ copies of the airtel exactly as they appear on the ELSUR cards. Except for required classification markings, as applicable, no additional notations are to be placed on this airtel (FD-664) to indicate the enclosed overhear cards relate to a source. The copy of this communication to be placed in the field office substantive file is to be redacted so as to reflect the symbol number of the source rather than the true name.

(h) ELSUR material is not to be indexed to nor submitted from an informant or asset file. ELSUR indexing is to be done reflecting the field office substantive case file.

(i) For additional instructions regarding informant or asset matters, see also Part I, Section 137, of this manual, or Part 1, Section 5, of the National Foreign Intelligence Program Manual.

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 84

EFFECTIVE: 10/16/96

10-10.6 Use of Consensual Monitoring in National Security Matters

Refer to Foreign Counterintelligence Manual, Appendix 1,  
Section IV.F.

EFFECTIVE: 12/05/85

10-10.7 Pen Registers (Dialed Number Recorder) (See MIOG, Part II,  
10-3, 10-10.11.3 & 16-7.4.6.)

(1) The Electronic Communications Privacy Act of 1986 (Act), as amended, regulates the use of dialed number recorders and the pen register technique (Title 18, USC, Sections 3121-3127). The Act codifies existing Department of Justice (DOJ) policy of obtaining a court order to authorize the installation and use of a pen register and sets forth the procedure for seeking such an order. It is not necessary to obtain a court order when the telephone user consents to the installation of the pen register device.

(2) Law enforcement agencies are required under Title 18, USC, Section 3121(c) to install and use technology that is "reasonably available" in order to limit the information obtained from a pen register to "the dialing and signalling information utilized in call processing" (only the numbers dialed to reach the called number, not additional numerical messages or codes). Such pen register technology is not now available. When technology is developed, the Engineering Section, Information Resources Division, will acquire and distribute same.

(a) Cell Site Simulators: This provision does not affect DOJ/FBI policy on the use of digital analyzers and cell site simulators. No court order is required to use these devices to acquire cell site data (cellular telephone ESN or MIN, or other facility-identifying information) when obtained without involving the telecommunication carrier or other intermediary. However, a pen register or trap and trace order is needed if these devices are used to obtain numbers dialed to or from a cellular telephone (i.e., call processing information).

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 85

Under Section 3121(c), a pen register order for a cellular telephone is limited to acquiring call processing information. Additional non-content information, such as cellular telephone ESN or MIN, cell site sector information, or other location type information may be considered "a record or other information pertaining to a subscriber" and obtained from a telecommunications carrier pursuant to a court order under Title 18, USC, Section 2703(d), or pursuant to a warrant or consent of the subscriber or customer.

(3) Supervisory personnel are to ensure that the use of the pen register is not substituted for other logical investigations. Prior to requesting that an attorney for the government apply for a pen register order under the Act, the case Agent should submit a memorandum or other appropriate communication, initialed by the supervisor, to the case file and to the pen register control file setting forth the reasons for pen register use and documenting the basis for the statements to be made in the application. If the United States Attorney or Strike Force Chief requires a written request specifying the factual basis for the assertions in the application, copies of the letter may be designated to the above-indicated files in lieu of a separate memorandum. The above instructions apply to all instances wherein a pen register is to be used, whether alone or in conjunction with the interception of wire or electronic communications under the provisions of the Act. A Division Counsel should be consulted if there is any question as to the sufficiency of facts stated or whether the existing facts are stated in a manner which would clearly warrant the assertions made in the application for the order. A copy of each order obtained must be filed in the pen register control file.

(4) Prior to the actual filing of an application for a pen register order, the case Agent is to ensure the availability of equipment within his/her field office. If the equipment is not available from the existing office inventory, then the TA or TTA should be requested to make appropriate contact with the Operational Support Unit, Information Resources Division, to secure equipment. All requests for pen register equipment must be confirmed in writing.

(5) The Act requires the Attorney General to make an annual report to Congress on the number of pen register orders applied for by law enforcement agencies of the Department. DOJ has advised the FBI by memorandum of this requirement and has requested quarterly reports on pen register usage. Court-ordered pen register usage must be reported to FBIHQ within five workdays of the expiration date of any original or renewal order. To satisfy DOJ data requirements and standardize and simplify field reporting, the form airtel captioned

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 86

"Pen Register/Trap and Trace Usage" (FD-712) must be used. If an order is obtained, but no actual coverage of any lines is effected, then no submission is required. These reporting requirements do not apply to pen register usage effected under the provisions of the Foreign Intelligence Surveillance Act.

(6) It should be noted that the same telephone line which carries the electronic impulses signaling the number which has been dialed also carries voice transmissions. Therefore, supervisory personnel must ensure that all FBI and non-FBI personnel operating pen register equipment solely under a pen register order be informed of the above and warned that audio monitoring equipment must never be utilized in connection with pen register coverage of telephone lines.

EFFECTIVE: 10/23/95

10-10.7.1 Emergency Provisions

If an emergency situation exists wherein time does not permit the obtaining of a court order for a pen register, any Deputy Assistant Attorney General or higher Department of Justice official may authorize the installation and use of a pen register prior to obtaining a court order. However, the specific provisions of Title 18, USC, Section 3125, must be satisfied. These provisions state:

(1) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any state or subdivision thereof acting pursuant to a statute of that state, who reasonably determines that -

(a) an emergency situation exists that involves -

1. immediate danger of death or serious bodily injury to any person; or

2. conspiratorial activities characteristic of organized crime,

that requires the installation and use of a pen register or a trap and

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 87

trace device before an order authorizing such installation and use can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such installation and use may have installed and use a pen register or trap and trace device if, within 48 hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with Section 3123 of this title.

(2) In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when 48 hours have lapsed since the installation of the pen register or trap and trace device, whichever is earlier.

(3) The knowing installation or use by any investigative or law enforcement officer of a pen register or trap and trace device pursuant to (1) above without application for the authorizing order within 48 hours of the installation shall constitute a violation of this chapter.

In essence, the "emergency" pen register provision mirrors the "emergency Title III" provision found in Title 18, USC, Section 2518(7). However, there are several differences. First, the number of statutorily designated DOJ officials who may approve emergency use of pen register devices in Federal investigations is broadened to include "any Assistant Attorney General, any Acting Assistant Attorney General, or any Deputy Assistant Attorney General." Second, unlike Section 2518(7), the emergency pen register statute does not include emergency situations involving "conspiratorial activities threatening the national security interest." In those rare situations where an "emergency" pen register would be required for use in situations threatening the national security, consideration should be given: (a) to utilizing the emergency provisions of the Foreign Intelligence Surveillance Act of 1978 (FISA), which regulates pen register devices as well as electronic surveillance interceptions in national security investigations, which include criminal espionage cases; or (b) to emphasizing that the situation, although threatening the national security, either involves an immediate danger of death or serious physical injury to any person or that the situation concerns conspiratorial activities characteristic of organized crime (e.g., a terrorist group's plan to bomb a building). Of course, if investigative or law enforcement officers are dealing with the telephone subscriber or customer (user), the customer's consent, as is indicated in Section 3121(b)(3), is sufficient, and a court order need

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 88

| not be obtained. |

EFFECTIVE: 01/22/90

| 10-10.8 Electronic Tracking Devices | (See MIOG, Part I, 7-14.6(15),  
9-7.1(2); II, 10-9.11(9), 10-10.11.1.) |

Electronic tracking devices, [REDACTED]  
are called beepers. The two devices must be distinguished from each  
other. This section addresses electronic tracking devices. [REDACTED]  
[REDACTED] Generally speaking, tracking  
devices are specifically excluded from Title III requirements because  
of the manner in which they function and the limited privacy  
implications related to their use (Title 18, USC, Section  
2510(12)(D)). However, in those circumstances where a court order is  
required, Title 18, USC, Section 3117 provides for extrajurisdictional  
effect. That is, a court order issued by a judge or magistrate may  
authorize the use of the device within the jurisdiction of the court  
and outside that jurisdiction if the device is installed in that  
jurisdiction. The Department of Justice has interpreted this section  
to mean that such use is valid outside of the court's jurisdiction  
both inside and outside the jurisdiction of the United States.

(1) On Vehicles

(a) A search warrant is not required to install an  
electronic tracking device on the exterior of a motor vehicle in a  
public place, and the device may be used to monitor the vehicle's  
travel over public roads. A person traveling in an automobile on  
public highways has no reasonable expectation of privacy in his/her  
movements from one place to another. Since no search or seizure is  
involved in the use of this technique, no quantum of proof is  
necessary to justify its use. Likewise, a search warrant is not  
needed to continue to monitor the device after the vehicle enters a  
private area, so long as the auto may be visually observed from  
adjoining premises. If the vehicle enters a private garage or hidden  
private compound, a search warrant should be obtained if monitoring is  
to continue.

(b) The same general rule has usually been applied  
to the use of tracking devices on aircraft.

(2) Other Personal Property

Sensitive  
PRINTED: 02/18/98

b2  
b7E



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 89

(a) Electronic tracking devices often are placed in various types of personal property and then used to monitor the location of the suspect and the property.

(b) Placement of an electronic tracking device inside personal property lawfully accessible to the Government is not a search under the Fourth Amendment. Likewise, monitoring the device while the property is in a public place, or open to visual observation, even though it is on private property, is not a search. However, monitoring the device once it has been taken into private premises not open to visual observation is a Fourth Amendment search which, in the absence of an emergency, requires a search warrant. It is not generally possible at the time of installation of an electronic tracking device to anticipate the route and the destination of the property into which it has been placed; and there exists a risk in any case that monitoring the device while it is located inside private premises will become necessary. Therefore, a search warrant should be acquired prior to the installation and monitoring of the device, unless an emergency exists which renders such acquisition impracticable. The application for the warrant should set forth (1) a description of the object into which the device is to be placed, (2) the circumstances justifying its use, and (3) the length of time for which the surveillance is requested. Because of the variety of situations in which electronic tracking devices may be employed and the need to maintain proper controls over their use, SAC authorization, with documented concurrence of the PLA and the AUSA, is required before such a device is utilized.

EFFECTIVE: 02/27/95

10-10.9 Closed Circuit Television (CCTV) (Video Only) - Criminal Matters (See MIOG, Part I, 9-7.2; II, 10-9.10(7), 10-10.1 (5).)

(1) Department of Justice (DOJ) regulations require that PRIOR AUTHORIZATION be obtained for all CCTV surveillances for law enforcement purposes. The level of such authorization will vary with the circumstances under which this technique will be employed.

(2) Authorization for the use of CCTV does not automatically convey authorization for the use of any other technique

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 90

(e.g., audio monitoring), either by itself or in conjunction with the use of this technique. The use of such additional techniques must be specifically requested at the proper level of authorization; must meet all requirements as set forth in this manual regarding the use of that technique; and must be specifically authorized prior to its use.

(3) A separate control file for CCTV matters should be established in each field office and appropriate documents relative to instructional material, authorization, and utilization of this technique should be retained. This control file will be for the purpose of the SAC's administrative control and for review during inspection.

EFFECTIVE: 05/08/95

10-10.9.1 CCTV Authorization - Criminal Matters (See MIOG, Part I, 9-7.2.)

It should be noted the use of HAND-HELD VIDEO RECORDERS is NOT to be confused with CCTV surveillance wherein the camera is placed in a remote location and generally concealed from view.

(1) For CCTV surveillance of events transpiring in public places, or places to which the public has general unrestricted access, and where the camera can be placed in a public area, or in an area to which the surveillance Agents have nontrespassory, lawful access, delegated FBI officials may independently authorize CCTV surveillance without the need to notify the DOJ either before or after the surveillance.

(2) All CCTV monitoring requires the approval of the SAC, following mandatory legal review and concurrence of the Chief Division Counsel (CDC). The SAC may authorize the use of CCTV for the duration of the investigation under the following circumstances:

(a) the CCTV camera is located in a public area or in a location under the exclusive possession and control of the FBI AND the area to be viewed is an exterior public area or an interior common area absent a reasonable expectation of privacy. Some examples are: (1) the CCTV camera is in a public area AND the area to be viewed is a public street or an exterior door; and (2) the CCTV camera is [REDACTED] AND the area to be viewed is a public hallway in a building or the

b2  
b7E

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 91

lobby of an apartment building, motel, bank or the like. The CDC should be consulted in all cases involving the nonconsensual monitoring of interior common areas to determine whether any circumstances exist which create an expectation of privacy.

(b) the CCTV camera is located on private premises, but no trespassory entry is required to install the equipment because consent to install has been obtained from a person with a possessory interest in the premises AND the area to be viewed is an exterior public area or an interior common area lacking an expectation of privacy; and

(c) in situations where there is nontrespassory or consensual placement of the CCTV camera and the area to be viewed is the interior of private premises or other areas where a reasonable expectation of privacy otherwise exists AND consent has been obtained from a participant in the activity to be viewed.

In cases which present sensitive or unusual circumstances the concurrence of the United States Attorney's Office (USAO) should also be obtained. (The opinion of the USAO, if required, shall be confirmed or obtained in writing.)

Before conducting CCTV surveillance outside of the division from which authorization is obtained, Agents must coordinate with and obtain concurrence from the SAC of each division where monitoring will occur. Such concurrence must be documented in writing by the office of origin if not documented by the lead office in the EC forwarding the recordings to the requesting office.

SAC authority to approve CCTV surveillance may not be redelegated. In the SAC's absence, however, individuals designated as "Acting SAC" may exercise the SAC's authority to approve CCTV surveillance under the above circumstances.

(3) Documentation of the above details, brief background concerning the investigation, and the authorization of the SAC must be set forth in the field office ELSUR Administrative Subfile to the substantive case file, with a copy designated for the field office CCTV control file. Form FD-677 (Documentation of SAC Authority for Closed Circuit Television (CCTV) Usage-Video Only) will be used for this purpose. In those cases involving sensitive or unusual questions or circumstances, the substantive desk at FBIHQ is to be notified.

(4) Video Surveillance where there is a Reasonable Expectation of Privacy. A court order is required for the use of CCTV

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 92

in ALL situations where a reasonable expectation of privacy exists either in the place where the camera is to be installed, or in the place to be viewed, and appropriate consent has not been obtained. If judicial authorization is required only for the installation of the camera (e.g., because the surveillance is of a public area or place where the public has unrestricted access, or because consent has been obtained from a participant in the activity to be viewed), prior DOJ approval is not required.

In ALL situations where there is a reasonable expectation of privacy in the area to be viewed and no consent has been granted, a court order and prior DOJ approval is required. CDC review and SAC approval of the CCTV affidavit and the concurrence of the respective AUSA or DOJ prosecutor is required prior to requesting DOJ approval. The application and order should be based on an affidavit that establishes probable cause to believe that evidence of a federal crime will be obtained through the surveillance, and should include:

- (a) a particularized description of the premises to be surveilled;
- (b) the names of the persons expected to be viewed, if known;
- (c) a statement of the steps to be taken to ensure that the surveillance will be minimized to effectuate only the purposes for which the order is to be issued;
- (d) a showing that normal investigative procedures have been tried and found wanting, or are too dangerous to employ; and
- (e) a statement of the duration of the order, which shall not be longer than is necessary to achieve the objective of the authorization, nor in any event longer than 30 days.

1. When CCTV is to be used IN CONJUNCTION WITH Title III aural surveillance, the affidavit supporting the aural surveillance may, if appropriate, also be used to support the video surveillance order. In such cases, DOJ policy requires a separate application and order prepared by the appropriate United States Attorney for the video surveillance, in addition to the usual application and order for aural surveillance.

2. See Part II, Section 10-9.10 of this manual for guidelines regarding Title III electronic surveillance.

Sensitive  
PRINTED: 02/18/98

Sensitive

(5) Documentation of Consent

(a) In those situations (i.e., nonpublic areas where a reasonable expectation of privacy exists) requiring the consent of an individual to view and/or video record, by use of CCTV equipment, any activity the consenting party may have, Agents should obtain written consent. This consent should be documented by executing FD-473a (Closed Circuit Television Consent) form whenever possible. However, oral consent will be acceptable in those instances where the consenting party declines to give written consent. When oral consent is obtained, at least two law enforcement officers (one of whom should be an Agent of the FBI) should be present to witness this consent, and the fact that the consenting party has declined to give written consent should be recorded on the FD-473a. This form should then be executed in all respects with the exception of the consenting party's signature.

(b) Form FD-473a should be executed and properly witnessed in all situations requiring consent for use of CCTV equipment, even when the consenting party is an informant, cooperative witness, Special Agent, or any other law enforcement officer. As in any case involving consensual monitoring, it is mandatory that the consenting party be present within the area to be viewed at all times when the CCTV equipment is activated.

(c) Consent should be obtained from both the participant in the activity being viewed and from the person or entity having possessory interest in the location where the equipment is to be placed or mounted, if the two individuals are not the same. Because of a wide variety of circumstances concerning installation of CCTV equipment, the CDC should be consulted in situations where any questions or any unusual circumstances arise.

(6) A substantial modification in either the location where the CCTV camera is to be placed or in the area to be subjected to CCTV surveillance, or a change in the primary subject(s) of the investigation, the anticipated target(s) of the CCTV surveillance, or the consenting party(s) will require separate authorization.

(7) All offices should ensure appropriate administrative controls are established.

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 94

EFFECTIVE: 09/17/97

10-10.9.2 CCTV - ELSUR Records - Criminal Matters

The use of nonaural CCTV (video only) in conjunction with a criminal investigation as outlined above does not constitute an "intercept" as defined in Title 18, USC, Section 2510, and, therefore, is technically not an electronic surveillance. As such:

(1) Absent other types of coverage, ELSUR cards relating to nonaural CCTV coverage are not to be prepared;

(2) Absent other types of coverage, a check mark should not be placed on the ELSUR line on case file covers and the file cover shall not be stamped "ELSUR."

(This situation does not apply to national security matters, as terminology defined by the Foreign Intelligence Surveillance Act of 1978 is different from that defined in Title III.)

EFFECTIVE: 12/10/93

10-10.9.3 CCTV (Audio and Video) - ELSUR Indexing - Criminal Matters

(1) CCTV to be used with the consent of a participant in conjunction with audio monitoring equipment may be handled in the same manner and in the same communication as a request for the consensual monitoring of nontelephone communications. See Part II, 10-10.3 of this manual entitled "Monitoring Nontelephone Communications in Criminal Matters," for procedures attendant to nontelephonic consensual monitoring usage.)

(2) For ELSUR indexing purposes, a microphone surveillance (MISUR) being used in conjunction with a CCTV surveillance will be treated as a MISUR.

(3) See Part II, 10-9.12, of this manual for ELSUR indexing requirements, procedures, and specific examples of principal, proprietary interest, and intercept records in Title III matters. In consensual monitoring matters, refer to Part II, 10-10.5, of this manual for indexing requirements, procedures, and specific

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 95

| examples of | intercept records. |

EFFECTIVE: 05/08/95

10-10.9.4 CCTV - Preservation of the Original Tape Recording

As with all original tape recordings, original CCTV recordings will be properly identified; duplicated, if necessary; placed in an FD-504 (Chain of Custody - Original Tape Recording) envelope; exhibited in the file; and otherwise maintained in accordance with standard instructions dealing with the handling of original tape recordings and the preservation of evidence.

EFFECTIVE: 09/22/87

10-10.10 Tape Recorders

(1) Heavy-duty plant-type recorders and portable single carrying case-type recorders, are usually utilized in court-authorized technical surveillance under Title III or the Foreign Intelligence Surveillance Act. (See Part II, |16-7.3.4, |of this manual relative to loan of this equipment to other law enforcement agencies.) Smaller handheld cassette tape recorders and concealable tape recorders are usually used for consensual monitoring. In either case the necessary authorization outlined in this manual must be obtained prior to their use for these purposes.

(2) Use of tape recorders for the purpose of overt recording of the statements of witnesses, suspects, and subjects is permissible on a limited, highly selective basis only when authorized by the SAC. To ensure the voluntariness of a statement electronically recorded, the following conditions are to be adhered to:

(a) the recording equipment must be in plain view of the interviewee;

(b) consent of the interviewee to the recording must be obtained and clearly indicated on the tape;

(c) the questioning must be carefully prepared so that the tone of voice and wording of the questions do not intimidate

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 96

or coerce; and

(d) recording tapes must not be edited or altered, and the originals must be sealed (in an FD-504, Chain of Custody - Original Tape Recording Envelope) and stored in such a manner as to ensure the chain of custody.

EFFECTIVE: 09/22/87

10-10.11 Radio Monitoring

EFFECTIVE: 09/22/87

10-10.11.1

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



XXXXXX  
XXXXXX  
XXXXXX

FEDERAL BUREAU OF INVESTIGATION  
FOIPA  
DELETED PAGE INFORMATION SHEET

1 Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

- Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552

Section 552a

(b)(1)

(b)(7)(A)

(d)(5)

(b)(2)

(b)(7)(B)

(j)(2)

(b)(3)

(b)(7)(C)

(k)(1)

(b)(7)(D)

(k)(2)

(b)(7)(E)

(k)(3)

(b)(7)(F)

(k)(4)

(b)(4)

(b)(8)

(k)(5)

(b)(5)

(b)(9)

(k)(6)

(b)(6)

(k)(7)

- Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.
- Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

Pages were not considered for release as they are duplicative of \_\_\_\_\_

Page(s) withheld for the following reason(s): \_\_\_\_\_

- The following number is to be used for reference regarding these pages:

M106- Part II Page 10-97

XXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X for this page X  
XXXXXXXXXXXXXXXXXXXX

XXXXXX  
XXXXXX  
XXXXXX

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 98

b2  
b7E



ELSUR indexing is required.

EFFECTIVE: 02/14/97

10-10.11.2 Cordless Telephones and Other Types of Radio  
Monitoring (See MIOG, Part I, 139-1.1.)

(1) Effective 10/25/94, with the passage of the Communications Assistance for Law Enforcement Act (CALEA), all cordless telephone conversations, including the radio portion of those conversations, are now accorded privacy protection under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III), Title 18, USC, Section 2510 ET SEQ. Prior to this legislation, the radio portion of many cordless telephone conversations could be monitored without a Title III or FISA court order. As a result of this amendment to Title III legislation, the monitoring of any cordless telephone conversation is subject to the same legal requirements as the monitoring of cellular telephones and traditional land line telephones. In the absence of consent, all such monitoring requires a Title III or FISA court order. For information regarding the investigation and use of unauthorized interceptions, see MIOG, Part I, Section 139 "INTERCEPTION OF COMMUNICATIONS" concerning violations of Title 18, USC, Section 2511.

(2) Certain other radio communications, such as those that are broadcast so as to be readily accessible to the public (AM and FM radio station broadcasts, unencrypted ship-to-shore communications, public safety communications, citizen band amateur and general mobile radio services, and the like) remain unaffected by the CALEA; as before, the interception of such communications does not require a Title III order. See Title 18, USC, Section 2511 (2) (g).

(3) Any additional questions regarding whether a particular device or radio communication is covered by Title III should be directed to the Investigative Law Unit, Office of the

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 99

General Counsel, FBIHQ.

EFFECTIVE: 06/03/96

10-10.11.3 Cellular Telephones

Both the wire and radio portions of a cellular telephone conversation are specifically covered by Title III and a Title III court order must be obtained to intercept cellular communications.

Noncontent information, such as cellular telephone ESN or MIN, cell site sector information, or other location type information may be considered "a record or other information pertaining to a subscriber" and, therefore, obtained from a telecommunications carrier pursuant to a court order under Title 18, USC, Section 2703(d), or pursuant to a warrant or consent of the subscriber or customer.

(1) Cell Site Simulators: No court order is required to use digital analyzers or cell site simulators (known as "triggerfish") to acquire cell site data (cellular telephone ESN or MIN, or other facility-identifying information) when obtained without involving the telecommunication carrier or other intermediary. However, a pen register or trap and trace order is needed if these devices are used to obtain numbers dialed to or from a cellular telephone (i.e., call processing information). (See MIOG, Part II, 10-10.7 "Pen Registers".)

(2) Access Device Fraud: The use of cellular telephones that are altered, or "cloned," to allow a fraudulent theft of service is now an illegal use of an access device under Title 18, USC, Section 1029(a), "Fraud and related activity in connection with access devices." This section specifically prohibits the use of an altered telecommunications instrument, or a scanning receiver, hardware or software, for purposes of obtaining unauthorized access to telecommunications services and defrauding the carrier. Section 1029 is a Title III predicate offense under Title 18, USC, Section 2516(c). Therefore, it allows the use of a Title III to obtain evidence of access device fraud.

EFFECTIVE: 10/23/95

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 100

10-10.12 Approval for the Use of Technical Equipment

Technical equipment shipped to field offices does not constitute authority for its use. In criminal matters, SAC, FBIHQ, or Department of Justice authorization is required prior to the use of certain types of electronic surveillance equipment. For the specific authorization required, in criminal matters refer to the appropriate section of this manual relating to the type of equipment being considered for use. In national security matters refer to the Foreign Counterintelligence Manual.

EFFECTIVE: 10/18/88

10-10.13 Technical Collection of Evidence - Safeguarding Techniques and Procedures

(1) Electronic Surveillance techniques must not be compromised by disclosure in correspondence and during judicial proceedings.

(2) Information regarding technical operations, equipment and techniques must not be divulged during testimony, in FD-302s, in Title III affidavits, or in other correspondence directed outside the FBI during the course of an investigation.

(3) This policy should be brought to the attention of all USAs and Strike Force Attorneys and other interested parties so that prosecutions can be planned without the necessity that the Government's case requires this type of disclosure.

(4) Details concerning the safeguarding of techniques and procedures and the testimony of TIAs can be found in Part II, Section 6 of this manual.

EFFECTIVE: 10/18/88

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 101

10-10.14 Review by Technical Advisor (TA)

All correspondence concerning technical matters is to be reviewed by the TA or, in his/her absence, a Technically Trained Agent (TTA) prior to being approved by the SAC or other official acting for SAC. The purpose of this requirement is to ensure that requests for technical matters are cleared through the individual in the office having the most current knowledge of equipment availability, equipment capability, technical procedures, and technical policies. The specific duties of the TTA are set forth in Part II, Section 16-7.2.6 of this manual.

EFFECTIVE: 10/18/88

10-10.15 Training for TTAs

(1) The TA will set minimum training requirements for all TTAs in TA's office and ensure that these minimum requirements are met. The minimum requirements will be different from office to office, but will be designed to provide all TTAs with experience in the provision of all aspects of electronic surveillance support.

(2) The SAC must ensure that a program for achieving minimum requirements is established and complied with consistently. The SAC must ensure that all communications, instructions, and SAC memoranda pertaining to technical work and technical equipment must be read and initialed by all active TTAs.

(a) The SAC will provide sufficient time for the TA to implement a program of instruction and training for active TTAs, investigative personnel, and supervisors.

(b) Additional information regarding Technical Training and the Technical Investigative Program can be found in Part II, Section 16-7 of this manual.

EFFECTIVE: 10/18/88

Sensitive  
PRINTED: 02/18/98

Sensitive

10-10.16

(1)

(2)

(3)

(4) Expert witnesses are available from the Technical Services Division, FBIHQ, for tape analysis and court testimony regarding authenticity relating to editing and other associated matters. These normally become points of question at pretrial hearings. It is a well-established fact that tape recordings and other technically collected evidence are admissible in court. On the basis of current case law, the Government can introduce tapes solely on the testimony of the Agent(s) who monitors and records the intercept (assuming the Agent can identify the voice(s) and testify to the authenticity of the tape).

b2  
b7E

Normally, the Agent who signs the application for a court-ordered intercept will be called as a witness at a suppression hearing.

(5) If, in an unusual circumstance, the Government's case mandates a disclosure of FBI technical operations, equipment or technique, the problem should be first brought to the attention of the Principal Legal Advisor who will determine the disclosure and the reasons. Alternatives to disclosure will be sought and if no

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 103

resolution is possible which would protect FBI technical concerns, then notification should be made to FBIHQ, Engineering Section, Technical Services Division, so a final decision can be made in conjunction with the appropriate FBIHQ investigative divisions.

(6) Further details as to 

b2  
b7E

EFFECTIVE: 01/22/90

10-10.17 Trap/Trace Procedures (See MIOG, Part I, 9-7(7), 91-11.3.2(1), & 192-14(1).)

(1) American Telephone and Telegraph (AT&T), other long line carriers and local operating telephone companies have the capability to identify a telephone number that is calling another specific telephone number through the use of trap and trace devices and procedures. This technique is an internal telephone company operation that can be successfully effected in certain limited circumstances.

(2) The Electronic Communications Privacy Act of 1986 (Act), as amended, regulates the use of this technique (Title 18, USC, Sections 3121-3127). The Act codifies existing Department of Justice (DOJ) policy of obtaining a court order to authorize the installation of a trap/trace device and sets forth the procedure for seeking such an order. It is not necessary to obtain a court order when the telephone user consents to the installation of a trap/trace device.

(3) DOJ and the FBI have reached agreements with AT&T and local telephone companies to follow certain guidelines in applying for and effecting the trap/trace technique. Investigative personnel requiring the use of this sensitive investigative technique should contact the field office Technical Advisor (TA) or a Technically Trained Agent (TTA) for information. Local trap/trace activity will be coordinated by the TTAs in the field office. (See Part II, 16-7.2.6(18) of this manual.)

(4) Supervisory personnel are to ensure that the use of a trap and trace is not substituted for other logical investigative measures. The case Agent should submit a memorandum or other appropriate communication, initialed by the supervisor, to the case file and to the trap and trace control file setting forth the reasons

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 104

for use of the technique and documenting the factual basis for certification to the court that the information likely to be obtained is relevant to an ongoing investigation, or in cases where the legal justification is based upon consent, documenting the consent of the user to the installation. If the United States Attorney or Strike Force Chief requires a written request specifying the factual basis for certification, copies of the letter may be designated to the above-indicated files in lieu of a separate memorandum.

The Chief Division Counsel should be consulted if there is any question as to the sufficiency of facts stated or whether the existing facts are stated in a manner which would justify the certification made in the application for the order. A copy of each order obtained must be filed in the trap and trace control file.

(5) The Act also requires the Attorney General to make an annual report to Congress on the number of trap/trace orders applied for by law enforcement agencies of the Department. DOJ has advised the FBI by memorandum of this requirement and has requested quarterly reports on court-ordered trap/trace usage.

(6) The use of court-ordered trap/trace techniques must be reported by airtel to FBIHQ, Attention: Operational Support Unit, Information Resources Division, within five workdays after the expiration date of each original or renewal order. To satisfy DOJ data requirements, and standardize and simplify field reporting, the form airtel captioned "Pen Register/Trap and Trace Usage" FD-712 must be used.

(7) These reporting requirements do not apply to trap/trace usage effected under the provisions of the Foreign Intelligence Surveillance Act.

(8) American Telephone and Telegraph (AT&T) and other carriers bill the FBI for costs associated with the installation of trap and trace devices and/or the utilization of trap and trace procedures. The cost of this technique varies considerably. The actual cost depends on the number of telephone company offices involved.

(a) Payment of these expenses follows the same guidelines as other areas of confidential expenditures, with SAC having authority to approve up to \$20,000 per case each fiscal year. Any requests over \$20,000 should be directed to FBIHQ, Attention: Operational Support Section, Criminal Investigative Division.



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 105

(b) Upon receipt of the monthly invoice/statement from AT&T, or other telecommunications carrier, FBIHQ conducts a preliminary review of all services that were provided and completed since the last billing period.

(c) Once the preliminary review is completed, a copy of the approved invoice/statement is forwarded with blank Form 6-153 to the appropriate field division which requested the service.

(d) Form 6-153 should be completed by the field division and returned to FBIHQ, Attention: Operational Support Section, Criminal Investigative Division.

EFFECTIVE: 02/14/97

10-10.17.1 Emergency Provisions

If an emergency situation exists wherein time does not permit the obtaining of a court order for a trap and trace, any Deputy Assistant Attorney General or higher DOJ official may authorize the installation and use of trap and trace procedures prior to obtaining a court order. However, the specific provisions of Title 18, USC, Section 3125, must be satisfied. These provisions state:

(1) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any state or subdivision thereof acting pursuant to a statute of that state, who reasonably determines that -

(a) an emergency situation exists that involves-

1. immediate danger of death or serious bodily injury to any person; or

2. conspiratorial activities characteristic of organized crime, that requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained, and

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 106

(b) there are grounds upon which an order could be entered under this chapter to authorize such installation and use may have installed and use a pen register or trap and trace device if, within 48 hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with Section 3123 of this title.

(2) In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when 48 hours have lapsed since the installation of the pen register or trap and trace device, whichever is earlier.

(3) The knowing installation or use by any investigative or law enforcement officer of a pen register or trap and trace device pursuant to (1) above without application for the authorizing order within 48 hours of the installation shall constitute a violation of this chapter.

In essence, the "emergency" trap and trace provision mirrors the "emergency Title III" provision found in Title 18, USC, Section 2518(7). However, there are several differences. First, the number of statutorily designated DOJ officials who may approve emergency use of trap and trace devices in Federal investigations is broadened to include "any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General." Second, unlike Section 2518(7), the emergency trap and trace statute does not include emergency situations involving "conspiratorial activities threatening the national security interest." In those rare situations where an "emergency" trap and trace would be required for use in situations threatening the national security, consideration should be given: (a) to utilizing the emergency provisions of the Foreign Intelligence Surveillance Act of 1978 (FISA), which regulates pen register/trap and trace devices as well as electronic surveillance interceptions in national security investigations, which include criminal espionage cases; or (b) to emphasizing that the situation, although threatening the national security, either involves an immediate danger of death or serious physical injury to any person or that the situation concerns conspiratorial activities characteristic of organized crime (e.g., a terrorist group's plan to bomb a building). Of course, if investigative or law enforcement officers are dealing with the telephone subscriber or customer (user), the customer's consent, as is indicated in Section 3121(b)(3), is sufficient, and a court order need not be obtained. Use Form FD-472 to document consent.

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 107

EFFECTIVE: 03/23/92

10-11 FBI UNDERCOVER ACTIVITIES - CRIMINAL MATTERS | (SEE MIOG,  
PART II, 10-14.1.5.) |

(NOTE: FBI UNDERCOVER ACTIVITIES - FCI MATTERS, SEE FCI  
MANUAL.)

~~The undercover technique is one of the most effective and successful investigative tools the Federal Bureau of Investigation has to investigate crime. As such, it should be protected and used wisely. The conduct of undercover operations (UCOs) is governed by the Attorney General's Guidelines (AGG) on FBI Undercover Operations which were initially approved in 1980 and revised 11/13/92. The FIELD GUIDE FOR UNDERCOVER AND SENSITIVE OPERATIONS which sets forth FBI policies and procedures concerning the conduct of UCOs has been disseminated to the field. The field office undercover coordinator (UCC) and the Undercover and Sensitive Operations Unit (USOU), Criminal Investigative Division, FBI Headquarters, should be consulted regarding specific questions relating to UCOs.~~

EFFECTIVE: 12/07/93

| 10-11.1 | Deleted |

EFFECTIVE: 10/18/93

| 10-11.2 | Deleted |

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 108

EFFECTIVE: 10/18/93

| 10-11.3 | Deleted |

EFFECTIVE: 10/18/93

| 10-11.4 | Deleted |

EFFECTIVE: 10/18/93

| 10-11.5 | Deleted |

EFFECTIVE: 10/18/93

| 10-11.6 | Deleted |

EFFECTIVE: 08/28/91

10-11.7 | Deleted |

EFFECTIVE: 08/28/91

| 10-11.8 | Moved and Renumbered as 10-16 |

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 109

EFFECTIVE: 08/28/91

| 10-11.9 | Deleted |

EFFECTIVE: 08/28/91

10-12 USE OF HYPNOSIS AS AN INVESTIGATIVE AID

---

EFFECTIVE: 02/16/89

10-12.1 Approval to Utilize (See MIOG, Part II, 10-3.)

Hypnosis is legally permissible when used as an investigative aid for lead purposes in Bureau cases where witnesses or victims are willing to undergo such an interview. The use of hypnosis should be confined to selective Bureau cases. Upon finding a willing witness or victim, Bureau authority must be obtained from the appropriate Assistant Director (AD) responsible for either the Criminal Investigative Division (CID) or the National Security Division (NSD), who may delegate this authority to their Section Chief designee. The Critical Incident Response Group's (CIRG's) Investigative Support Unit (ISU) functions as a technical resource to the field and must receive copies of all communications pertaining to the use of hypnosis. Set forth in your request for authorization the name of the hypnosis expert you intend to use and a brief summary of the expert's qualifications. You should consider using a psychiatrist, psychologist, physician, or dentist who is qualified as a hypnotist. Those with forensic training are preferred. If there are no qualified or reliable hypnotists available, the ISU should be contacted to obtain the name of a qualified hypnotist nearest your field division. Upon receipt of Bureau authority, the matter must be thoroughly discussed with the USA or Strike Force Attorney in Charge. Include the fact that the case Agent or the SAC's designee will attend the hypnotic session, and advise whether that person is likely to participate in the hypnotic session. The use of hypnosis on a witness must have the concurrence of the Assistant United States Attorney (AUSA) in that district, as well as the approval of the AD, CID or NSD, as appropriate, or their substantive Section Chief designee. You are cautioned that under no circumstances will Bureau personnel

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 110

participate in hypnotic interviews in non-Bureau cases.

EFFECTIVE: 03/21/96

10-12.2 Hypnotic Session

(1) It is recommended that written permission to conduct a hypnotic interview be obtained prior to the interview. This permission should include permission of the witness or victim to have ~~the entire hypnosis session audio or video taped or both.~~

(2) It is important that you either audio or video tape the entire session and any subsequent hypnotic sessions. Video tape, however, is the preferred method of recording these sessions.

(3) When considering the use of hypnosis, one important aspect is the proper prehypnotic explanation of this technique to the witness or victim. Hypnosis is not a product of the power or magic of the hypnotist. The witness or victim is not likely to reveal his or her innermost secrets or lose control of his or her mind. Further, hypnosis itself is not likely to produce any physical or psychological damage to the person hypnotized.

(4) You must also bear in mind that the use of the information obtained through hypnosis cannot be assumed to be necessarily accurate. Careful investigation is needed to verify the accuracy of information obtained during these sessions.

EFFECTIVE: 02/16/89

10-12.3 Role of Case Agent in Hypnotic Session

The case Agent will act as liaison with the hypnotist and will attend the hypnotic session. If the case Agent cannot attend, an SAC-approved designee will handle the duties of the case Agent. It must be clearly understood that the hypnotist is charged with the responsibilities of conducting and supervising the hypnotic session, and must remain physically present throughout the proceedings. With the PRIOR CONCURRENCE AND GUIDANCE of the hypnotist, the case Agent may question the witness or victim under

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 111

| hypnosis, |but will not conduct the hypnotic induction or terminate the hypnotic state. The request for authorization to utilize hypnosis will include the name of the |case Agent or designee|who is acting as liaison.

| |The|number of persons actually present at the hypnotic session should be held to a minimum.

EFFECTIVE: 07/17/95

10-12.4 Hypnosis Evaluation

In order to evaluate the efficacy of this technique, a detailed summary describing the results of the hypnotic interview must be forwarded to the Bureau with a copy to |the Critical Incident Response Group's (CIRG's) Investigative Support Unit (ISU).| This summary should specifically include the following items:

- (1) The identification of any significant investigative information obtained through the utilization of this technique.
- (2) Total number of hypnosis sessions to include the length of each session.
- (3) The hypnotic technique utilized to include the manner of recording the interview.
- | (4) The identity of the |case Agent or SAC designee|and the hypnotist.
- (5) Disposition of the case.

EFFECTIVE: 07/17/95

Sensitive  
PRINTED: 02/18/98

Sensitive

10-13 VISUAL INVESTIGATIVE ANALYSIS (VIA)

The Visual Investigative Analysis Unit's primary objective is to assist the investigator by graphic analyses of all information and physical evidence (toll records, pen register records, financial records, etc.) related to significant and complex investigations. The VIA Unit utilizes an information management data base to achieve this objective. The data base allows for data retrieval by chronology and/or subject matter. The analytical models derived from this data base include VIA Networking, Link Analysis and Matrix Analysis.

(1) VIA Networking is a case management technique which assists in the planning, coordinating, controlling and analyses of complex investigations. It displays chronological relationships among known and alleged activities related to a crime and the dependent relationship of investigation to those activities. Link Analysis graphically displays individual and organizational relationships among all entities identified during the investigation. It demonstrates these relationships by utilizing various types of lines to illustrate the strength of the relationships, and geometric figures to differentiate persons, places, assets, organizations and other aspects of the investigation. Matrix Analysis, a complementary technique, summarizes factors related to a series of crimes to identify similarities. The analytical models reconstruct the crime and related investigation, and demonstrate the complicity of suspects/subjects. They are supported by written reports that contain observations of the analyst, based on the analysis of available information. The results of the VIA process provide investigative and prosecutive personnel with a basis for developing future investigative and prosecutive strategy.

(2) Should a field office desire Investigative Support Information System (ISIS) support and anticipate using VIA, the VIA assistance should be requested at the same time as the ISIS support. This will allow ISIS and VIA personnel to structure the ISIS data base to make it compatible with the VIA application.

(3) Since the primary objective of VIA is to assist the investigation, requests for VIA assistance should be sent to the VIA Unit, Criminal Investigative Division, as early as possible during the investigation and should include a synopsis of the investigation.

EFFECTIVE: 11/20/90



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 113

10-14 ADVANCE FUNDING FOR INVESTIGATIVE PURPOSES | (See MAOP, Part II, 6-11, 6-12, & 6-12.3(3).) |

(1) | Appropriated funds are available directly from FBIHQ for investigative purposes in situations where the expenditure is of a confidential nature. An advance of funds may be requested to fund confidential case expenditures which cannot be readily supported from the field office draft system. Such expenses include the purchase of evidence such as drugs, payments to cooperating witnesses, and other large nonrecurring items. Advance of funds shall be used to fund all Group I Undercover Operations. NOTE: Group I Undercover Operation advances MAY NOT be used to fund drug purchases or cooperating witness/criminal informant expenses. Field offices may also request an advance of funds for Foreign Counterintelligence Undercover Operations, Special Operations Groups, Off Premise Sites, Special Surveillance Groups, and Show and Buy-Bust requirements.

(2) Once an advance of funds has been received from FBIHQ to fund an investigation, SAC authority to spend funds from the draft system is rescinded. The draft system may no longer be used until all advances have been liquidated or returned and appropriate authority to use the draft system has been obtained. |

EFFECTIVE: 12/07/93

10-14.1 Types of Advance Funding Authority

Funds may be requested for the following investigative purposes:

EFFECTIVE: 11/23/87

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 114

10-14.1.1 Case Authority

(1) The SAC has authorization to spend up to \$20,000 per fiscal year for confidential expenditures incurred in connection with any single investigative matter, including Group II Undercover Operations (see paragraph (3) below). SAC authority in the amount of \$20,000 is automatically renewed for each case at the beginning of each succeeding fiscal year, unless advised to the contrary by FBIHQ. If expenditures are projected to exceed SAC authority of \$20,000 during the fiscal year, a request for additional authority must be sent to the appropriate substantive program manager at FBIHQ to request **ADDITIONAL AUTHORITY** for the amount of expenditures that are anticipated for the remainder of the fiscal year. Each request must include:

- (a) That additional case authority is requested for a specific amount.
- (b) Detailed justification to support the request.
- (c) Total amount spent to date during the investigation, regardless of the source of funds.
- (d) Statement as to the availability of funds in the field office budget. If the balance of available budgeted funds is insufficient to support planned expenditures, the authority request must include a request to reallocate funds from another budget category or a request to supplement the total field office budget.
- (e) Adequacy of the draft system to fund request.
- (f) A deadline by which FBIHQ must respond.
- (g) Wire transfer instructions if expeditious handling is required. Wire transfers less than \$25,000 must be justified.

(2) If additional authority is approved, the date upon which the additional authority was granted **MUST** be noted on each advance or expense request in excess of \$20,000.

(3) The SAC may approve nonsensitive undercover operations (Group IIs) with maximum cumulative funding of \$40,000 for operational expenses. The SAC may not, however, authorize spending of

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 115

more than \$20,000 in such matters. As explained above, if expenditures are projected to exceed \$20,000 during a fiscal year, a request for additional authority must be made of the substantive program manager at FBIHQ, in conformance with procedures set forth in paragraph (1) above.

EFFECTIVE: 12/07/93

~~10-14.1.2 Informant Payment Authority (See MIOG, Part II, 10-14.1.3, & MAOP, Part II, 6-11.).~~

An advance of funds may be requested to pay informants for information provided. Payment is based on the value of the information and is approved on a payment-by-payment basis. The SAC is authorized to approve cumulative payments up to \$20,000. Additional payments or individual payments in excess of \$20,000 must be approved at FBIHQ. Requests for authority to make a payment or requests for an advance of funds to make a payment should be directed to FBIHQ and should contain the following:

- (1) Justification for the payment
- (2) Adequacy of the draft system to fund the payment
- (3) Justification of the "emergency" if a wire transfer has been requested.

EFFECTIVE: 12/07/93

10-14.1.3 FCI/Terrorist Informant Authority

An advance of funds may be requested for regular monthly payments to FCI/Terrorist informants for information being provided. Authority for such payments can only be granted by FBIHQ. Requests for authority and advances of funds should be set out as described for Informant Payment Authority in 10-14.1.2 above.

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 116

EFFECTIVE: 12/07/93

#### 10-14.1.4 Bribe of Public Officials Authority

Advances may be made for bribe payments. Authority to attempt bribes of public officials should be obtained pursuant to policy defined in Part I, 58-6.6(1) and 194-5.6(1) of this manual. Requests for advances of funds should be made to the substantive desk at FBIHQ, and should contain the following information:

(1) Adequacy of the draft system to provide the bribe money

(2) Justification of the "emergency" if a wire transfer is requested.

EFFECTIVE: 12/07/93

#### 10-14.1.5 Undercover Funding Authority (See NFIPM, Part 1, 7-1.11.)

Request for advance funding for FCI, Group I and Group II Undercover Operations should be made to the substantive desk at FBIHQ. Short-term FCI and Group II Undercover Operations may be funded from the draft system. Larger FCI and Group II cases may use advanced funds if the draft system is insufficient to fund the operation. All Group I Undercover Operations are funded from FBIHQ advances. Authority to conduct undercover operations is discussed in Part II, 10-11, of this manual, "FBI UNDERCOVER ACTIVITIES - CRIMINAL MATTERS." Authority to conduct undercover operations in FCI matters is discussed in the NATIONAL FOREIGN INTELLIGENCE PROGRAM MANUAL (NFIPM).

EFFECTIVE: 02/14/97

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 117

10-14.1.6 Show and Buy-Bust Money Funding Authority

(1) Show and Buy-Bust money is available on a case-by-case basis to provide financial credibility for an asset/informant, cooperating witness or Undercover Agent or to consummate a proposed illegal transaction in support of a specific investigative case. Use of these funds does NOT constitute an EXPENDITURE of appropriated funds. Such funds are NEVER to be allowed to become evidence or to leave the care, custody or control of the FBI. They are to be returned to FBIHQ when no longer needed by the case for which their use was originally authorized so that they may be subsequently reissued.

(2) Show funds cannot be deposited into a bank or other financial institution without an exemption from the Attorney General. Upon receipt of an exemption, the funds are to be placed in a federally insured financial institution, unless otherwise authorized, to provide credibility to an operation.

(3) The funds may be used in a display of cash to reinforce the role of an Undercover Agent or to consummate a proposed illegal transaction as part of an arrest (Buy-Bust) scenario.

(4) The SAC may approve the use of up to [REDACTED] for Show purposes or for use in a Buy-Bust situation. The use of more than [REDACTED] must be approved in advance by FBIHQ. b2, b7E

(5) Requests for Show or Buy-Bust funds must specify:

(a) Justification for the use of the funds and the need for Attorney General exemptions for the use of bank account(s),

(b) That the United States Attorney will not require the funds to be retained as evidence,

(c) That the funds will not be allowed to leave the care, custody or control of the FBI, and

(d) Precautions to be taken to ensure the safety of involved personnel and the security of funds to be used.

(6) Show and Buy-Bust funding requests in amounts of [REDACTED] or less should be sent directly to the attention of the Confidential Services Unit, Accounting Section, Finance Division, (copy to the FBIHQ substantive desk for information) with the personal approval of the SAC or, in SAC's absence, the ASAC. b2  
b7E

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 118

(7) All Buy-Bust funding requests and requests for Show money in amounts of more than [REDACTED] should be directed to the substantive desk at FBIHQ.

b2, b7E

EFFECTIVE: 12/07/93

10-14.1.7 Deleted

EFFECTIVE: 05/25/90

10-14.2 Delivery of Advance

Funds can be made available to the field by Department of the Treasury check or, in the case of an emergency, by wire transfer. All advances of appropriated funds are made to specific cases and cannot be commingled with advances for other cases. All requests must be submitted under the investigative case caption with a complete field office file number. The funds may not be deposited in any bank without an exemption from the Attorney General.

(1) Department of the Treasury Check - Once a request for an advance is approved by the substantive desk it takes three working days for the Accounting Section to obtain a check from the Department of the Treasury. The check, which is payable to the SAC, is then forwarded to the field by airtel. Requests should be made far enough in advance to anticipate time for the approval process, acquisition of the check, and delivery by the U.S. Postal Service.

(2) Wire Transfer - An approved request for an advance by wire transfer received by the Accounting Section by [REDACTED] will usually be delivered in the field by [REDACTED]. Requests for wire transfers should contain the following information:

b2,  
b7E

(a) Name and address of receiving bank (must be a Federal Reserve System Member Bank)

(b) Name and title of bank contact

(c) Official Bureau name of the Special Agent who will pick up the funds. (See MIOG, Part I, 58-6.6(1) &

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 119

| 194-5.6(1.) |

EFFECTIVE: 12/07/93

10-14.3 Accountability/Vouchering Requirements

When an office requests an advance of funds from FBIHQ the SAC assumes the responsibility for providing adequate resources to safeguard the advance and to account for it in a timely fashion. The field is to verify the outstanding balances of all advances except Show Money as of the last day of each month. The certification will take the form of a Confidential Travel Voucher (SF-1012) and is due at FBIHQ by the tenth day of the following month. A Confidential Travel Voucher is required for each calendar month an advance is outstanding even if no expenditures were made during a given month, because the "no amount" voucher serves to certify the cash balance outstanding at the end of each month.

(1) Physical Responsibility - Funds are advanced to a specific office for use in a specific case. They are tracked by field office file number. The funds advanced for one case or office cannot be utilized by another case or office. The SAC is personally responsible for all advances sent to SAC's division. The advance will remain SAC's responsibility until the funds are returned to FBIHQ or the expenditures of the funds are reported to FBIHQ on a Confidential Travel Voucher with a Blue Slip (FD-37) supported by paid receipts or Agent certifications for each and every expenditure.

(2) Confidential Travel Voucher - All expenditures from advances of appropriated funds are to be vouchered promptly on a Confidential Travel Voucher (SF-1012). Vouchering procedures are described in the CONFIDENTIAL FUNDING GUIDE; however, the following general rules apply:

(a) Expenditures must be vouchered promptly and no less frequently than monthly.

(b) A voucher must be submitted for each calendar month that the advance remains outstanding.

(c) The voucher should represent that calendar month's expenditures.

Sensitive  
PRINTED: 02/18/98

Sensitive

(d) The amount reported on line 8 (d) "Balance Outstanding" on the SF-1012 must represent the cash on hand on the last day of the calendar month being reported.

(e) For the purpose of certifying the balance of cash on hand, a voucher must be submitted even for months in which no expenditures were made.

(f) Vouchers are due at FBIHQ by the tenth day of the month following the month being reported.

(g) The Confidential Travel Voucher is supported by a Blue Slip (FD-37) and both must be signed by the SAME approving official, either the SAC or ASAC.

(h) The voucher must be supported by original paid invoices (receipts) or signed certifications for each and every expenditure included in the voucher and listed on the itemization of expenditures.

(i) An Itemization of Expenditures (FD-736) and a Voucher Reconciliation (FD-735) must be attached to the voucher.

(3) Return of Funds to FBIHQ - Advances no longer needed for the case for which they were advanced should be sent back to FBIHQ as soon as possible. They can be returned by check or wire transfer.

(a) Return by Check - Outstanding balances of less than \$25,000 are to be returned by cashier's check payable to the FBI. The check should be attached to the final voucher listing expenditures for the month in which the outstanding funds are being returned. The returned funds should be described (e.g., "return of direct advance," "return of show money," "submission of interest income," "refund of deposit," etc.) in the Voucher Reconciliation (FD-735) attached to the voucher. Costs incurred in purchasing cashier's checks or money orders must be vouchered as expenditures, not deducted from the amount to be remitted.

(b) Return by Wire Transfer - Outstanding balances of \$25,000 or more should be returned to FBIHQ by wire transfer.

1. The funds should be wired from a Federal Reserve System Member Bank through the Treasury Financial Communication System (TFCS) to:

Department of the Treasury - Federal Reserve Bank,



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 121

New York City, Treasury Department Code [REDACTED]  
for credit to [REDACTED]

b2

2. The bank should also be instructed to include in the third party information section of the TFCS funds transfer message format, a description of the return in the following format:

Field office abbreviation and field office file number, name of the remitting Agent and the statement, "Return of outstanding balance of advanced funds." (e.g., "BS 183G-1224, SA John Smith, Return of outstanding balance of advanced funds.")

NOTE: DO NOT include classified file numbers in the TFCS transfer message format.

(4) On the same day the funds are wired, a teletype must be sent to FBIHQ, Accounting Section, Attention: Confidential Services Unit, confirming the wire transfer and describing the type of funds being returned, i.e., return of a direct advance, show money, interest income, or evidence.

(5) The final voucher, listing expenditures for the month in which the outstanding funds are being returned, must be submitted to the Confidential Services Unit, Accounting Section. The returned funds should also be described (e.g., return of advanced funds, show money, etc.) on the Voucher Reconciliation (FD-735) attached to the voucher.

EFFECTIVE: 12/07/93

10-14.4 Field Office Centralized Control System for Advance of Funds

As with all advances to field offices, advances for investigative purposes must be reported to and included in the field office centralized control system for advance of funds. This requires that one copy of the Bureau communication confirming an advance of funds be placed in a 66F- control file captioned "Advance of Funds Control File." In addition, a ledger page must be created for each advance received. The ledger will record the amount received, vouchers submitted against the advance, any funds returned, the date of cash counts, and internal audits. Instructions as to the operation

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II.

PAGE 10 - 122

of the centralized control system can be found in the MAOP, Part II, 6-12, "Advance of Funds - Centralized Control System."

EFFECTIVE: 12/07/93

10-15 TRACING OF FIREARMS

Firearms that are recovered during and subsequent to FBI investigations and/or other documentary evidence of firearms, both foreign and domestically manufactured, should be traced through the appropriate district office of the Bureau of Alcohol, Tobacco and Firearms (ATF), when possible and consistent with FBI interests. Furnish the type of firearm, including the manufacturer, model, caliber or gauge, barrel length, overall length, serial number, and name and address of interested U.S. Attorney (USA). If certification is needed for court proceedings, this will be furnished directly to the interested USA by ATF, per Part I, Section 4, if this manual, entitled "Firearms Acts."

EFFECTIVE: 08/28/91

10-16

[REDACTED]

[REDACTED]

[REDACTED]

Sensitive  
PRINTED: 02/18/98

Sensitive

[REDACTED]

b2  
b7E  
[REDACTED]

EFFECTIVE: 08/28/91

10-17 FBI INVESTIGATIVE INFORMATION SERVICES DATA BASES FOR USE  
IN INVESTIGATIONS

(1) The FBI has hundreds of investigative information data base services available to its personnel through the Butte Information Technology Center and the Savannah Information Technology Center (ITC). These investigative information support services are useful in all FBI investigations, especially in locating witnesses and fugitives, identifying personal and corporate asset records, and generating lead information. There are Technical Information Specialists (TIS) on site in both centers, 24 hours a day, seven days a week.

(2) The information available is automated and may vary by state according to how it is collected, stored and retrieved. Requests for services from the ITCs may be submitted telephonically on the Forms FD-809 or FD-809A. The method of request (phone, fax, or mail) and the assigned precedence dictate the priority of the request. The average response time for routing requests is within two days; for priority requests is within 24 hours; and for immediate requests is within two hours. Immediate requests made by telephone are handled at once and the results returned by telephone within minutes. The TIS analysts provide all the information retrieved to the Agent along with a brief synopsis of that information. Attached to each response returned by the ITCs is a reply form (FD-810) for quality assurance and accomplishments. Please ensure that this reply form is returned to the ITCs.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 124

(3) All field offices have access to and should utilize the "Telephone Application" (on the FBINET), a central repository for telephone subscriber data. The data in the "Telephone Application" should be checked prior to setting leads for telephone-related records.

(4) Field offices should check the ITCs and the FBINET before setting leads to other offices.

(5) The following is a sample of the types of information of data bases currently available through the ITCs:

(a) On-line automated "criss-cross," directory-type information access for information on names of individuals or businesses, telephone numbers and subscriber information, and addresses for a subject or the neighbors of a subject.

(b) CREDIT RECORD HEADER INFORMATION - Credit Record Header information provides SKIP/TRACE, ADDRESS UPDATE, Social Security Account Number (SSAN) information, and other personal or business locator information based on name, social security number, or address information.

(c) ASSET INFORMATION - Information concerning

b2  
b7E

[REDACTED]

and news service libraries. Professional licensing information from some states, and deceased SSAN information is also available. Asset information is not available in an automated format for every county in every state.

(d) INFORMATION TO VERIFY SOCIAL SECURITY NUMBERS - Provides information regarding SSANs. A given SSAN can be checked to see if it falls with the range of active account numbers, approximately when it was issued, and from what state.

Information from the Social Security Administration on SSANs that have been reported as deceased, including the name that the SSAN was issued to, the address where the last death benefit was mailed, and the month and year of death.

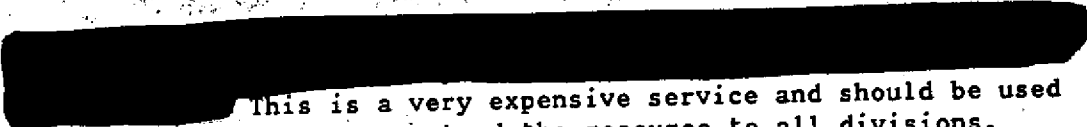
(e) [REDACTED]

b7D

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 125

 This is a very expensive service and should be used prudently so that we may extend the resource to all divisions. b7D

(f) NATIONAL INSURANCE CRIME BUREAU (NICB) - Provides information based on vehicle, fire, property, and casualty insurance claims. Also, information is available on the date and place that a vehicle was manufactured and where the vehicle was first shipped, based on the vehicle identification number. This information is a prerequisite to determine federal jurisdiction for certain offenses such as carjacking. Such information can be obtained in an affidavit form or if necessary, an expert witness from NICB can provide testimony at trial.

(g) NCIC/NLETS/CCH - This is the same service available in all field offices and should still be searched routinely in the field office; however, for offline searches, fugitive investigations, and when specifically requested, the ITCs will have the capability to access this information.

(h) TECS II - Treasury Enforcement Communications System II provides information collected by U.S. Customs Agents, Treasury Agents, and Immigration and Naturalization Service Agents in the course of their investigations. This information can be searched by name and by various identification numbers. Border crossings into the United States may also be searched by individual's name and by vehicle license number or aircraft registration number.

(i) 

(j) SENTRY - Bureau of Prisons on-line information system. Sentry has information on all inmates incarcerated in federal institutions since 1981. Available information includes admissions, transfers, housing, and work histories.

(k) FEDERAL TRADE COMMISSION - TELEMARKETING FRAUD DATABASE - Provides information on complaints received from the National Association of Attorneys General, Telemarketing Fraud Database. This information allows the aggregation and consolidation of complaints nationwide.

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 10 - 126

EFFECTIVE: 03/13/97

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 1

SECTION 11. TECHNIQUES AND MECHANICS OF ARREST

11-1 ARREST TECHNIQUES

EFFECTIVE: 05/10/82

11-1.1 General

(1) It is the responsibility of all SACs to plan arrests carefully and thoroughly. Each arresting operation should be in hands of an experienced Agent on those occasions when there is justifiable reason for SAC not personally participating in arrest.

(2) A person who is being placed under arrest may do one of several things: submit peacefully; attempt to flee; attempt to injure or kill arresting person; commit suicide; effect a rescue by confederates. Arresting party should consist of enough Agents/officers, whenever possible, to cope properly with those or other situations which might arise.

(3) Person arrested should be aware of intention of arresting Agent to deprive him/her of his/her liberty by legal authority. It is the duty and responsibility of arresting Agent to identify himself/herself in a clear, audible voice as a Special Agent of the FBI.

(4) Agents in making arrests are expected to be firm, to take proper precautions for their own safety, and to meet force with sufficient force to subdue any opposition.

(5) No definitive policy can be promulgated on firearms use in arrest situations. Good training and experience in arrest situations must be relied on to provide the proper response when confronted with deadly force situations. There are many situations in which Agent personnel may draw their weapons when making an apprehension and without being confronted with existing deadly force. This is a judgment question, which must be evaluated in terms of the individual or individuals to be apprehended, and the circumstances under which the apprehension is being made.

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 2

EFFECTIVE: 05/10/82

11-1.2 Initial Approach

(1) The first conversation with a person under arrest is extremely important and will enable such person to judge the ability of the Agent at the time of the arrest. A person under arrest should be made to understand that Agents will demand prompt and absolute obedience. Unnecessary conversation should be avoided. It is the responsibility of the arresting Agent to inform a person under arrest of the charges against him/her. ~~The language used in explaining the charge and offense should not be in greater detail than the language appearing in the body of the warrant.~~ Prisoners have been known to use many ruses in an effort to destroy evidence or to effect an escape following their arrest. Prisoners should not be granted personal privileges immediately following arrest and immediate requests for water, cigarettes, and permission to go to the lavatory before being searched should be denied. If, due to the circumstances, prisoners are to be transported long distances, common sense and good judgment should dictate the personal privileges granted.

(2) In making arrests on the street, the approach should always be made from the side or rear when possible. The person to be arrested should be arrested away from intersections and crowds when possible.

Experienced criminals realize that if it is possible for them to break away from an officer and run into a crowd they may effect an escape successfully. Arresting Agents, when appropriate, should wear their badges in such a manner as to display immediately their authority if challenged either by a police officer or a citizen.

(3) When a person is arrested, he/she should not be permitted to move about, unless authorized by arresting Agents. If it is necessary to obtain clothing for a person under arrest, Agents should inquire as to the location of the clothing so that it may be obtained by an Agent. Such clothing should be carefully searched prior to delivery to the prisoner.

EFFECTIVE: 05/26/89

Sensitive  
PRINTED: 02/18/98



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 3

11-1.3 Search of the Person

EFFECTIVE: 05/26/89

11-1.3.1 Preliminary Search

(1) At the time a person is arrested by Agents or voluntarily comes to an office and information is developed from him/her resulting in his/her arrest, such person must be adequately searched for concealed weapons which could be used for committing suicide or attacking another person. The search should be made, as much as reasonably possible, in a way that will not frustrate such person's cooperation with the Agents. It should be remembered, however, that safety is the primary factor and it takes precedence when the subject is not cooperative. Continuous suitable observation and guarding of such persons, dependent upon the circumstances, should be followed.

(2) Sound judgment should be exercised in compliance with (1) above. It may be inadvisable to make a preliminary search of a prominent citizen at the time of his/her arrest in the presence of his/her employees, customers, or friends unless such person is known to be potentially dangerous. Even under these circumstances, however, before transporting such an individual to the nearest U.S. Magistrate, he/she must still be adequately searched for concealed weapons and Agents may consider the privacy of a nearby office or other available area for this purpose. Under no circumstances should an arrested person ever be transported in a Bureau vehicle without being searched for weapons.

(3) The SAC, or in SAC's absence, the ASAC, shall be immediately notified of the presence in an office of any person under arrest or of the presence of any suspect for whom arrest is contemplated.

(4) Information on the law on search and seizure is contained in the Bureau document, "Search of the Person." (See also Legal Handbook for Special Agents, Section 5, captioned "Search and Seizure.")

(5) During the search of an arrested person, caution should be exercised by Agents coming into immediate contact with such individuals. Firearms should be handled in such a manner that will prevent the person under arrest from forcibly gaining possession of

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 4

them.

(6) When an Agent and a cooperating law enforcement officer find it necessary to provide a preliminary search of a person, the Agent should be the searcher.

EFFECTIVE: 05/26/89

11-1.3.2 Final Search and Collection of Evidence

(1) A preliminary search, even though believed to be thorough, cannot be relied upon as being adequate. Where possible, a more thorough final search of an arrested person should be conducted as soon as possible. Under existing Bureau instructions, the final search will usually be conducted in a place of local detention. Wherever possible, Agents should assist local authorities making the final search to ensure thoroughness and the securing of any additional evidence the subject may have on his/her person. In conducting a final search of an arrested person, possibilities of attempting self-destruction, escape, or concealment of additional weapons and evidence should be considered. To search a person thoroughly, his/her clothing should be removed and each article of wearing apparel carefully examined, as well as all portions of his/her nude body. Criminals are known to carry two or more concealed weapons and the finding of one firearm or weapon through a preliminary search may not indicate that the person is disarmed.

(2) While searching for weapons, particular attention should be given pencils and fountain pens which may prove to be tear gas weapons. Care should be exercised in handling this type of weapon which is considered dangerous.

(3) Fugitives very often conceal money on their persons in an effort to smuggle it into prisons or penitentiaries for the purpose of using it as bribes. They are oftentimes very ingenious in this respect and unless a careful search is conducted the money may be overlooked. Money has been concealed in belts; belt buckles; fountain pens; the lining of clothing; in the tongues, heels, and under the innersoles of shoes; in bandages; in artificial limbs; in the bottom of metal containers and matchboxes; in the prisoner's mouth; in the crotch; in pocket flaps; in shoulder padding; in concealed pockets; in outer and inner hat bands; sewed in suspenders; in necktie knots; in cap visors; in wristbands; and fastened to the soles of his/her feet or under the armpits with adhesive tape. Hack saw

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 5

blades have been concealed in shoe soles, coat lapels, and sewed in the back of a vest.

(4) Any article having thickness should be inspected with suspicion and every square inch of a prisoner's clothing and body should be carefully examined.

(5) Such articles as notebooks, newspaper clippings, and keys may be the source of valuable leads. The prisoner should be required to account for all notations and addresses in notebooks or on other articles and should be questioned as to the use of each key.

(6) Evidence and weapons should be displayed to another Agent immediately upon removing them from a prisoner so that both Agents can testify as to their source. Care should be exercised in the handling of large sums of money and, when feasible, should be counted in the presence of the arrested person and one other Agent.

(7) Firearms should not be carelessly unloaded, but the cartridges should be marked and sufficient notations made to enable an Agent to testify as to the exact condition of the gun at the time of its removal.

(8) Serial numbers of firearms obtained in connection with Bureau cases should be searched through the National Crime Information Center (NCIC). Whenever possible, any vehicles, property, currency, securities, traveler's checks, or money orders in possession of an individual arrested in Bureau cases should be searched through NCIC unless the source of the vehicles, property, etc., is known.

(9) Two or more Agents shall conduct the search and a complete descriptive and itemized list in duplicate shall be made of all articles removed from his/her person. Erasures or corrections shall be initialed by the prisoner.

EFFECTIVE: 05/26/89

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 6

11-1.4 Transportation of Arrested Persons

(1) Transportation of persons under arrest is primarily the responsibility of the U.S. Marshal's office. It will usually be necessary for Agents to transport persons arrested from the place of arrest to the place of local detention. In certain instances, it may be necessary for the arresting Agents to take an arrested person before the nearest U.S. Magistrate. Particularly this is true where the arrest is made in a city or metropolitan area wherein there is located a U.S. Magistrate. When more than one subject is transported in an automobile, it is desirable to place the subjects in the rear seat of the car. With one subject and two or more Agents, one Agent should ride in the rear seat with the subject. This Agent should be seated directly behind the driver. With only one Agent present and one subject, extreme caution should be taken to ensure the subject is securely handcuffed and closely supervised when placed in the vehicle. The use of the subject's or Agent's belt to secure the handcuffs to the person in front or rear and the use of the seat belt are additional methods of controlling the subject. If any delay is anticipated with regard to transportation of the arrested person or his/her timely appearance before a U.S. Magistrate, it is the responsibility of the arresting Agents to communicate immediately with the SAC for instructions.

(2) When an arrest is made at a considerable distance from a U.S. Magistrate, the U.S. Marshal's office may be unable promptly to transport such arrested person. Each SAC should have a clear understanding with the U.S. Marshal's offices within the office territory concerning the procedure to be followed in such instances and this procedure should be made known to all Agents assigned to the field office.

(3) Care should be taken in all cases in which confessions and signed statements are obtained to avoid any delay in hearings before U.S. Magistrates which would bring the case within the purview of the McNabb and Mallory decisions.

EFFECTIVE: 05/26/89

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 7

11-1.5 Handcuffing

Agents are fully responsible for the welfare and condition of a person once he/she is placed under arrest, and it is required that all arrested persons be handcuffed with hands behind the back, back to back, and double locked. If circumstances necessitate handcuffing with the hands to the front, then the hands must be back to back, and the cuffs must be belted down and double locked. Agents are reminded that handcuffs and other restraining devices are only temporary controls and Agents must maintain a close guard over subjects at all times until they are released to another authority.

EFFECTIVE: 05/26/89

11-2 PROCEDURES FOR ARREST

EFFECTIVE: 05/26/89

11-2.1 Arrests and Searches

EFFECTIVE: 05/26/89

11-2.1.1 Types of Arrest Warrants

There are two forms of warrants for the arrest of Federal law violators.

(1) Magistrate's warrant - issued by the USMAGISs based upon a complaint.

(2) Bench warrant - issued by the clerk of the U.S. district courts following the return of an indictment or the filing of an information on an order of the district judge.

EFFECTIVE: 05/26/89

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 8

11-2.1.2 Authority to Serve Arrest Warrants

(1) While U.S. Marshals are authorized to execute all lawful writs, process, or orders issued under the authority of the U.S. Courts, including criminal warrants, Rules 4(a)(1) and 9(c)(1) of the Federal Rules of Criminal Procedure state arrest warrants also may be executed by some other officer authorized by law. FBI Agents are so authorized.

(2) FBI Agents are authorized and should serve all arrest warrants issued in cases over which the FBI has investigative jurisdiction. While every effort should be made to use only FBI Agents in apprehending subjects for whom an arrest warrant has been issued, based on the exigency of the situation the Special Agent in Charge (SAC) may authorize joint arrests with state and local authorities, U.S. Marshals, or other Federal law enforcement agencies (See Part II, Section 21-28 of this manual). Special concern should be given to the utilization, or at least the alerting, of local authorities in instances where it may logically be anticipated that resistance could be forthcoming from the subject(s) or member of the community. Although the time of notification to local authorities concerning arrests made within their jurisdiction by FBI Agents is being left to the discretion of the SACs, concern must be given to the sensitivity of our associates in local law enforcement to know what is transpiring in their jurisdictions and we must respect their responsibility to the people of their communities.

(3) In executing an arrest warrant, which is accomplished with the apprehension/arrest of the subject, the Agent need not have the warrant in his/her possession at the time of arrest. Upon request, however, he/she should show the warrant to the defendant as soon as possible. If the officer does not have the warrant in his/her possession at the time of the arrest, he/she shall then inform the defendant of the offense charged and of the fact that a warrant has been issued. Where time will permit and the successful arrest of subject will in no way be jeopardized, the arresting Agent should have the warrant of arrest in his/her possession in order that the same may be exhibited to the subject upon request.

EFFECTIVE: 05/26/89

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 9

11-2.1.3 Summons and Subpoenas

(1) Summonses should not be served by Bureau Agents or Investigative Assistants except upon authority of FBIHQ.

(2) The summons shall be served upon a defendant by delivering a copy to defendant personally, or by leaving it at defendant's dwelling house or usual place of abode with some person of suitable age and discretion then residing therein and by mailing it to the defendant's last known address.

(3) In situations where it would be clearly advantageous to the outcome of the case for Agents and/or Investigative Assistants to serve subpoenas the SACs are authorized to permit Special Agents and/or Investigative Assistants to serve subpoenas. SACs are to follow such matters closely to ensure judicious use is made of this authority.

EFFECTIVE: 05/26/89

11-2.1.4 Arrests Without Warrants

(1) Authority and Notification -

(a) When the facts and exigency of the situation demands, FBI Agents are authorized to make an arrest without a warrant. If time permits, however, every effort should be made to obtain the approval for such arrest from the SAC and USA.

(b) In situations where good judgment would command that FBIHQ be notified of an office's obtaining authorization to arrest an individual without a warrant, such notification must be given. Otherwise, a timely communication to FBIHQ of such arrest will suffice.

(2) Emergency Situations -

(a) Wherever possible prosecution should be authorized and a warrant issued prior to an arrest. In Bureau cases, in emergency situations, an arrest without warrant may be made for any Federal offense committed in the presence of FBI Agents, or for any felony cognizable under the laws of the United States where there are reasonable grounds to believe that the person to be arrested has committed or is committing such felony. Reasonable grounds or

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 10

reasonable cause is the same as "probable cause."

(b) Where an arrest has been made without prior authorization of prosecution and without a warrant in emergency situations, the USA or in USA's absence the AUSA must be contacted immediately for authorization of prosecution and arrangements made for the hearing before the nearest USMAGIS without unnecessary delay as provided for under rule 5(a) of the Federal Rules of Criminal Procedure.

(3) Misdemeanors - Arrest without warrant in misdemeanors within the Bureau's investigative jurisdiction may be made only where the offense is actually committed in the presence of the FBI Agents.

(4) Instructions Contrary to Bureau Regulations - Where instructions are received from USA or his assistant for arrest and detention of a Bureau subject in any manner contrary to Bureau rules and regulations, such instructions are not to be complied with in absence of FBIHQ authority. On receipt of such instructions, FBIHQ should be promptly advised.

EFFECTIVE: 05/26/89

11-2.1.5 Forcible Entry

In making an arrest Agents have authority to break outer and inner doors of a dwelling if the entry is made in good faith and with reasonable cause to believe that the person to be arrested is within the premises. But notice must first be given of authority and purpose, with a demand for admission, and a refusal.

EFFECTIVE: 01/31/78

Sensitive  
PRINTED: 02/18/98



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 11

11-2.1.6 Search of the Person (See also Legal Handbook for Special Agents, 5-3.5.)

Officers have an unquestioned right to search the person of one lawfully arrested. Anything found, including all documents and papers, may be taken. "The person" includes a package, bag, or satchel being carried. Searches of body cavities are permissible where (a) the searching Agent has probable cause to believe evidence of a crime is concealed in a body cavity, (b) the search of the cavity is made by trained medical personnel using medically sound procedures, (c) a search warrant or court order is obtained unless consent is given or emergency circumstances exist, and (d) only such force as is necessary and reasonable is used to effect the search.

EFFECTIVE: 06/28/94

11-2.2 Custody of Prisoners

EFFECTIVE: 01/31/78

11-2.2.1 Other Than District of Prosecution

(1) Upon the written request of a Special Agent of the FBI, the marshal is authorized to take custody of a prisoner notwithstanding the fact that the warrant or other court papers are not in his possession and to take the arrested person without unnecessary delay before the nearest available U.S. Magistrate to secure a temporary mittimus pending receipt of the outstanding warrant or other court papers. The written request to the marshal is to be signed by a Special Agent and shall include the name of the person arrested, the Federal charge upon which he is being held, and the district in which the warrant is outstanding. It shall also indicate whether or not directions have been given for the forwarding of the warrant to the arresting marshal.

(2) Form FD-351 may be used to request the marshal to assume custody of a prisoner. Since this form also provides spaces for data concerning details of the process issued, a copy of FD-351 may be sent to the USA and the U.S. Magistrate for information and

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 12

necessary action.

(3) If, due to emergency conditions, the marshal is unable to comply with the request of an Agent, the Agent should follow a reasonable course, and if circumstances dictate, handle the necessary transportation or arraignment accordingly.

EFFECTIVE: 01/31/78

11-2.2.2 Property of Prisoner

When a person under arrest is released to the custody of a U.S. Marshal or other law enforcement officer, all property that is to be returned to or accompany such person shall be delivered to the U.S. Marshal or other law enforcement officer in the presence of the person under arrest. An itemized receipt should be obtained. Weapons or property held as possible evidence shall not be released in this manner but shall be disposed of as provided for under existing instructions.

EFFECTIVE: 01/31/78

11-2.2.3 Removal of Prisoner from the Custody of the U.S. Marshal

(1) Removal of prisoner from the U.S. Marshal's custody for interviews when necessary by Agents requires authority of SAC and certification in writing to the U.S. Marshal.

(2) Interviews with prisoners as provided for above should be conducted only when absolutely necessary. Every precaution should be exercised in safeguarding such prisoners interviewed in field offices.

(3) Where prisoners are removed from the custody of the U.S. Marshal under the provisions of this section and transported to some place other than a field office for the purpose of re-enacting the scene of a crime or for the purpose of aiding in the location of a hideout, etc., prior FBIHQ authority is necessary before making a request of the U.S. Marshal's office for the release of the prisoner.

(4) "No agent or employee of the Government or any law enforcement officer shall have the right to remove a prisoner awaiting

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 13

trial from the place of detention without an order of the court or permission from the Bureau of Prisons, except that whenever a United States Attorney or an Agent in Charge of a local office of the Federal Bureau of Investigation of the Department of Justice, duly identified, certifies in writing that a prisoner awaiting trial cannot properly or conveniently be interviewed at the place of detention, and that public interest requires a temporary removal therefrom and requests in writing that such prisoner awaiting trial be brought from the place of confinement to the office of the United States Attorney or to the office of the Federal Bureau of Investigation in the same city, such request shall be honored whenever practicable. In such case the prisoner shall be returned to the place of detention within twenty-four hours after his removal therefrom.

"In the case of such absence from the jail, notice thereof on prescribed Form No. D.C. 4ld should promptly be sent to the United States Marshal for the judicial district in which the jail is located.

"No sentenced prisoner shall be removed without the approval of the Bureau of Prisons."

(5) There is set forth hereafter form D.C. 4ld which should be used as notice to the U.S. Marshal of removal of any Federal prisoner for the purposes mentioned:

REPORT OF TEMPORARY RELEASE OF PRISONER

This is to certify that on \_\_\_\_\_ at \_\_\_\_\_ (Hour) at the request of \_\_\_\_\_ (Name of D.A. or Agent) I removed Federal prisoner \_\_\_\_\_ from \_\_\_\_\_ at the office of \_\_\_\_\_ and returned him the same day at \_\_\_\_\_ in accordance with the provisions of Circular No. 2676-AA.

(U.S. Marshal or Deputy) \_\_\_\_\_

(Jud. Dist.) \_\_\_\_\_

EFFECTIVE: 05/10/82

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 14

11-2.3 Miscellaneous

EFFECTIVE: 05/10/82

11-2.3.1 Requests of Incarcerated Subjects

In all cases in which a Bureau subject is incarcerated either prior to or after arraignment and plea, if the subject makes known to an Agent during the course of an interview or otherwise |his/her|desire to be brought before the district court judge or to see a U.S. Marshal, immediate steps should be taken by the Agent to advise the USA or U.S. Marshal of the desires of the subject.

EFFECTIVE: 05/10/82

11-2.3.2 Medical Attention for Bureau Subjects

When any person in Bureau custody complains of sickness or ill health or where such condition is reasonably apparent to Agents present, arrangements should be made to afford such persons medical attention without delay.

EFFECTIVE: 05/10/82

11-2.3.3 Arrest of Foreign Nationals

(1) Within U.S. Territory - In every case in which a foreign national is arrested by the FBI, inform the foreign national that |his/her|consul will be advised of |his/her|arrest unless |he/she| does not wish such notification to be given. If the foreign national does not wish to have |his/her|consul notified, the arresting officer shall also inform |him/her|that if there is a treaty in force between the U.S. and |his/her|country which requires such notification |his/her|consul must be notified regardless of |his/her|wishes and that any necessary notification of |his/her|consul will be made by the USA. In all arrests by the FBI of foreign nationals (including those where the foreign national has stated that |he/she|does not wish |his/her|consul to be notified), the FBI field office shall inform the nearest USA of the arrest and of the arrested person's wishes regarding consular notification.

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 15

(2) Outside U.S. Territory - Agents have no jurisdiction in foreign countries. Within limitations border office Agents may, through liaison with cooperative foreign agencies in adjacent countries, arrange for investigations to be conducted. This should be done in a circumspect manner to avoid any allegation of violation of the sovereignty of the foreign country. Agents cannot be present at the scene of arrests by foreign authorities, participate in or be present during searches incidental to such arrests, accompany foreign officials transporting prisoners, or interview such prisoners except at their place of incarceration in the presence of foreign authorities. Where official business requires more than two days in a foreign country, authority must be obtained from FBIHQ.

EFFECTIVE: 05/10/82

11-3 ROADBLOCKS

EFFECTIVE: 05/10/82

11-3.1 General

(1) Several situations may arise which will require that one or more roads be blocked.

(2) Consider utilization of roadblocks in cooperation with local and state law enforcement agencies in cases in which such action appears to be logical.

(3) The SAC should be cognizant of the state and local laws regarding the utilization of roadblocks. Arrangements should be worked out with pertinent local law enforcement agencies for establishment of roadblocks and for transmission to surrounding local and state police.

EFFECTIVE: 05/10/82

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 16

11-3.2 Roadblock Methods

There are set forth below several suggestions as to effective means of blocking roads.

(1) To block roads for the purpose of inspecting automobiles. To block persons who may be leaving a particular area most effectively.

[REDACTED]

b2  
b7E

Wooden barricades and stop signs can be utilized in telling the vehicles to travel in one lane. Several cars should be permitted to pass through one direction and then several from the other direction so that the traffic will not be unduly delayed.

[REDACTED]

(2)

[REDACTED]

b2  
b7E

If the car turns around and attempts to turn back, the Agents in the first car can use their car to block the road.

(3) In general, the type of barricade used will depend upon the type of highway, the amount of traffic on it, the surrounding terrain, the character of the persons sought, and the time available.

[REDACTED]

b2  
b7E

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 17

[REDACTED]

[REDACTED] (4) [REDACTED]

b2  
b7E

(5) Whenever a roadblock is established in which any Bureau personnel are physically present and participate, it is fundamental that the Agents be in charge of such operation and they must make sure that the police or any others participating furnish fuel cooperation. Each SAC will be held personally responsible to see that any such roadblock is complete. In planning a roadblock, definite consideration must be given to providing for the safety of the officers participating and innocent citizens who can logically be expected to run into such a roadblock on the public highway.

EFFECTIVE: 05/10/82

11-4 RAIDS

EFFECTIVE: 05/10/82

11-4.1 SAC Responsibility

(1) When a dangerous assignment arises in which the practical application of firearms might be reasonably anticipated, the SAC must personally take charge. SACs must assume leadership in raids or arrests where firearms might be used and in major cases of great importance even though there is no indication that firearms might be employed. Unless emergency conditions prevent prior notification, the SAC or person acting in his absence must be immediately notified when such a situation arises, before action is taken toward apprehension. FBIHQ should be advised by teletype or telephone of the name of the official who will be in charge of the dangerous assignment. If the SAC or ASAC will not be on the spot in charge, sufficient explanation should be outlined which will indicate the reasons for the inability of the above-named official's participation.

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 18

(2) If a major case is being investigated involving the hot pursuit of fugitives which requires a concentration of Agents, it is incumbent upon each SAC to arrange for 24-hour coverage in the resident agencies in his territory where the activity is such that it can be expected there will be numerous phone calls and contacts from cooperative citizens and other law enforcement personnel. Where necessary, clerks may be utilized to effect such coverage. No such coverage should be initiated without authority from FBIHQ.

EFFECTIVE: 05/10/82

11-4.2 Elements of a Raid

A raid is an offensive type of operation characterized by the suddenness of its delivery. The purpose of conducting raids is usually to apprehend individuals or search premises. No two raids if planned to best advantage will be conducted exactly the same. However, the following elements will characterize well-planned operations of this type:

- (1) Speed.
- (2) Surprise.
- (3) Simplicity.
- (4) Safety of all personnel.
- (5) Superiority of manpower and firepower.

EFFECTIVE: 05/10/82

11-4.3 Planning Raids

EFFECTIVE: 05/10/82



11-4.3.1 Raid Commander and Responsibilities

(1) Every raid should be carefully planned in advance to ensure the greatest factor of safety to the residing party and innocent bystanders, and to prevent the escape of the persons sought.

(2) One individual designated as a raid commander should be responsible for planning and conducting of the raid, and it is his/her responsibility to see that all members of the raiding party are aware of the parts they are to take in the raid and he/she alone should be charged with the duty of changing plans and issuing orders as the situation may demand.

(3) [REDACTED]

(4) [REDACTED]

(5) [REDACTED]

b2  
b7E

EFFECTIVE: 05/10/82

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 20

11-4.3.2 Selection and Composition of the Raid Party

[REDACTED]

(1) [REDACTED]

b2  
b7E

(2) [REDACTED]

EFFECTIVE: 05/10/82

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 21

11-4.3.3 Raid Orders

Raid orders are issued by the raid commander who will advise each Agent or officer on the raid of his/her specific duty. He/She will, of course, furnish all of the information available concerning the persons to be apprehended to the members of the raiding party.

EFFECTIVE: 05/10/82

11-4.3.4 Equipment

[REDACTED]

b2  
b7E

EFFECTIVE: 11/26/84

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 22

11-4.3.5 Assembly Location

(1)

[REDACTED]

(2)

[REDACTED]

b2  
b7E

(3) Since the success of a raid depends upon secrecy and surprise, every effort should be made to avoid having the pre-raid plans and movement come under the scrutiny of outside persons or organizations not immediately involved or associated with the operation.

EFFECTIVE: 11/26/84

11-4.4 Approach to Raid Site

(1)

[REDACTED]

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 23

[REDACTED]

(2)

[REDACTED]

b2  
b7E

EFFECTIVE: 02/20/90

11-4.5 Entering the Place to be Raided

EFFECTIVE: 02/20/90

11-4.5.1 Identification of Raid Party

(1) Raids may begin by a signal from the raid commander to the occupants of the place being raided, advising them of the official identity of the raiding party and requesting their surrender. Sometimes this can be accomplished by a telephone call and in other instances it will be necessary to shout to the occupants of the house from the outside. Many raids of premises, however, are begun by the raid commander, after providing for appropriate outside protection of the premises, approaching the front entrance and demanding entry after making his/her presence and official capacity known.

(2) In any raid the participants should clearly identify themselves as Special Agents of the Federal Bureau of Investigation to all persons in the place being raided and those nearby so that no claim can be made by subjects that they were being hijacked by other gangsters. Identity should be made known verbally by a loud clear statement on the part of the raiding officers that "We are FBI Agents," or "We are Special Agents of the FBI," and by display of badges. Identity of an Agent may not immediately be given under the following circumstances:

(a)

[REDACTED]

b2  
b7E

(b)

[REDACTED]

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 24

(c) [REDACTED]

b2  
b7E

EFFECTIVE: 02/20/90

11-4.5.2 [REDACTED]

[REDACTED]

EFFECTIVE: 02/20/90

11-4.5.3 [REDACTED]

[REDACTED]

EFFECTIVE: 05/20/94

11-4.6 The Covering Party

EFFECTIVE: 02/20/90

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 25

11-4.6.1 Duties of the Covering Agents

(1) [REDACTED]

(2) When persons are seen emerging from the house, they should be advised of the raiders' identity and called upon to surrender. If, however, they come out of the house shooting, the covering Agents should immediately return fire.

(3) [REDACTED]

(4) [REDACTED]

(5) [REDACTED]

b2  
b7E

EFFECTIVE: 02/20/90

11-4.7 Post Raid Responsibilities

EFFECTIVE: 02/20/90

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 26

11-4.7.1 Arrest of Subjects

All persons identified as subjects and subsequently arrested during the course of a raid should be removed from the premises and appropriate security precautions taken to prevent escape or rescue attempts. Subjects are to be properly advised of their rights.

EFFECTIVE: 02/20/90

11-4.7.2 Raid Site Security

[REDACTED]

b2  
b7E

EFFECTIVE: 02/20/90

11-4.7.3 Publicity

All raids should be conducted as discreetly as possible and without resulting in undue publicity. The names of participants in a raid should not be disclosed without prior FBIHQ authority. Should anyone be killed during a raid and inquest by local authorities is necessary, arrangements can usually be made for one or two Agents to testify for the entire raiding party.

EFFECTIVE: 01/22/90

11-4.8 Miscellaneous

While participating in a raid, Agents should be alert to the need for "fire discipline" and exercise caution and good judgment when discharging weapons.



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 27

EFFECTIVE: 01/22/90

11-4.9 Photograph of Subjects

Photographs of Bureau subjects should be taken before blank walls with no Bureau equipment, pictures, or other Bureau material showing. The use of identifying numbers or name cards is recommended. The subject's name, description, date photograph taken, office name and case number, and, if known, subject's FBI number should be listed on the reverse side of the photograph. The field office case number must be shown in the "OCA" block on the subject's fingerprint card. Previously, photographs were sent to the Criminal Justice Information Services Division, either separately or attached to the fingerprint card. Photographs are not to be submitted. If a photograph of a Bureau subject is taken, simply check the appropriate block (yes or no) on the back of the fingerprint card indicating whether or not a photograph of the subject is available, and file the photograph in the 1-A section of the field investigative file. Should the Criminal Justice Information Services Division receive a request for the photograph, the requestor will be directed to the appropriate field office. Remember to show the field office investigative file number in the "OCA" block on the fingerprint card as this number will be quoted to agencies desiring the subject's photographs. Juveniles may not be fingerprinted or photographed without the written consent of the court unless the juvenile is prosecuted as an adult. (See Part II, 13-7.1.2 of this manual for further photographing information.)

EFFECTIVE: 04/08/96

11-5 EMERGENCY AND PURSUIT DRIVING

(1) Emergency driving describes the need to move by motor vehicle from one place to another in an expeditious manner in order to respond to exigent circumstances. Pursuit driving refers to the following of a motor vehicle for the purpose of making an apprehension or conducting a surveillance. Both emergency and pursuit driving may require tactics or techniques which increase the risks already inherent in operating a motor vehicle.

(2) FBI vehicles responding to emergency or pursuit

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 11 - 28

situations will utilize an adequate warning system, such as a siren, flashing light, or other device required by local statutes where use of such equipment will not defeat the FBI's mission. While employing such devices, drivers of Bureau vehicles during an emergency or a pursuit continue to have a duty to drive with due regard for the safety of others.

(3) In the interest of safety, the following factors should be considered prior to initiating maneuvers or speed which could pose a risk of death or serious injury to participants or third parties:

(a) The seriousness of the offense under investigation including whether the suspect has threatened the life or safety of others or poses a risk to the community in the event of escape.

(b) Variables such as the weather, road conditions, performance capabilities of the vehicles involved, and the presence of pedestrians and other traffic.

The above factors should be communicated to the driver's supervisor as soon as it is practical to do so. If, in the judgment of the driver or the supervisor, the potential risks outweigh the benefits to be derived from continued pursuit or emergency response, such pursuit or response should be terminated. The use of a vehicle or roadblock to effectuate a stop can be considered a seizure under the Fourth Amendment and must be conducted in a reasonable manner and in conformity with FBI policy concerning the use of force as set forth in the Legal Handbook for Special Agents, 3-6.4.

EFFECTIVE: 01/22/90

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 1

SECTION 12. FIREARMS

12-1 AUTHORIZATION AND RESPONSIBILITY TO CARRY FIREARMS (See  
MAOP, Part II, 2-1.5 & Legal Attache Manual, 2-18.)

|Special Agents (SAs) of the Federal Bureau of  
Investigation are authorized|to carry firearms under Title 18, USC,  
Section 3052.

EFFECTIVE: 04/07/97

12-1.1 SAC Responsibility

SACs are ultimately responsible for the use and  
maintenance of all firearms and related equipment in their respective  
divisions. SACs are also responsible for|providing training in  
firearms to all personnel authorized to carry weapons on official  
duty.| A Principal Firearms Instructor (PFI) will be assigned by the  
SAC to manage the|field|firearms|training|program.

EFFECTIVE: 04/07/97

12-1.2 Special Agent (SA) Responsibility (See MAOP, Part I,  
1-3.2.)

|SAs are directly responsible for|the appropriate use,  
security|and maintenance of|all|firearms and related equipment under  
their control.

EFFECTIVE: 04/07/97

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 2

12-2 UTILIZATION OF FIREARMS

EFFECTIVE: 05/20/94

12-2.1 Deadly Force - Standards for Decisions (See MIOG, Part II, 30-3.8 (3); MAOP, Part I, 1-4 (4); LHBSA, 3-6.4 & 4-2.5.) (Formerly at 12-2.1.1)

(1) POLICY TEXT:

(a) DEFENSE OF LIFE - Agents may use deadly force only when NECESSARY, that is, when the Agents have probable cause to believe that the subject of such force poses an imminent danger of death or serious physical injury to the Agents or other persons.

(b) FLEEING SUBJECT - Deadly force may be used to prevent the escape of a fleeing subject if there is probable cause to believe:

1. the subject has committed a felony involving the infliction or threatened infliction of serious physical injury or death, and

2. the subject's escape would pose an imminent danger of death or serious physical injury to the Agents or other persons.

(c) VERBAL WARNINGS - IF FEASIBLE, and if to do so would not increase the danger to the Agent or others, a verbal warning to submit to the authority of the Agent shall be given prior to the use of deadly force.

(d) WARNING SHOTS - No warning shots are to be fired by Agents.

(e) VEHICLES - Weapons may not be fired solely to disable moving vehicles. Weapons may be fired at the driver or other occupant of a moving motor vehicle only when the Agents have probable cause to believe that the subject poses an imminent danger of death or serious physical injury to the Agents or others, and the use of

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 3

deadly force does not create a danger to the public that outweighs the likely benefits of its use.

(3) DEFINITIONS

(a) Deadly Force: Force that is likely to cause death or serious physical injury.

(b) Necessity: In evaluating the NECESSITY to use deadly force, two factors are relevant: 1) The presence of an IMMINENT DANGER to the Agents or others; and 2) The ABSENCE OF SAFE ALTERNATIVES to the use of deadly force. Deadly force is never permissible under this policy when the sole purpose is to prevent the escape of a suspect.

1. Imminent Danger: "Imminent" does not mean "immediate" or "instantaneous," but that an action is pending. Thus, a subject may pose an imminent danger even if he/she is not at that very moment pointing a weapon at the Agent. For example, imminent danger may exist if Agents have probable cause to believe any of the following:

a. The subject possesses a weapon, or is attempting to gain access to a weapon, under circumstances indicating an intention to use it against the Agents or others; OR,

b. The subject is armed and running to gain the tactical advantage of cover; OR,

c. A subject with the capability of inflicting death or serious physical injury--or otherwise incapacitating Agents--without a deadly weapon, is demonstrating an intention to do so; OR

d. The subject is attempting to escape from the vicinity of a violent confrontation in which he/she inflicted or attempted the infliction of death or serious physical injury.

2. Absence of a safe alternative: Agents are not REQUIRED to use or consider alternatives that increase danger to themselves or to others. If a safe alternative to the use of deadly force is likely to achieve the purpose of averting an imminent danger, deadly force is not necessary. Among the factors affecting the ability of Agents to SAFELY seize a suspect, the following are relevant:

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 4

a. RESPONSE TO COMMANDS - Verbal warnings prior to using deadly force are required WHEN FEASIBLE--i.e., when to do so would not significantly increase the danger to Agents or others. While compliance with Agents' commands may make the use of deadly force unnecessary, ignoring such commands may present Agents with no safe option.

b. AVAILABILITY OF COVER - Availability of cover provides a tactical advantage. An armed suspect attempting to gain a position of cover may necessitate the use of deadly force; conversely, an Agent in a position of cover may gain additional time to assess the need to use deadly force without incurring significant additional risks.

c. TIME CONSTRAINTS - The inherent disadvantages posed by the issue of action/reaction, coupled with the lack of a reliable means of causing an instantaneous halt to a threatening action, impose significant constraints on the time-frame in which Agents must assess the nature and imminence of a threat.

(3) APPLICATION OF DEADLY FORCE

(a) When the decision is made to use deadly force, Agents may continue its application until the subject surrenders or no longer poses an imminent danger.

(b) When deadly force is permissible under this policy, attempts to shoot to cause minor injury are unrealistic and can prove dangerous to Agents and others because they are unlikely to achieve the intended purpose of bringing an imminent danger to a timely halt.

(c) Even when deadly force is permissible, Agents should assess whether its use creates a danger to third parties that outweighs the likely benefits of its use.

EFFECTIVE: 04/07/97

| 12-2.1.1 | Revised and Moved to 12-2.1 |

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 5

EFFECTIVE: 04/07/97

| 12-2.1.2 | Revised and Moved to 12-2.2 |

EFFECTIVE: 04/07/97

| 12-2.1.3 | Revised and Moved to 12-2.3 |

EFFECTIVE: 04/07/97

| 12-2.2 | Carrying of Weapons | (See also MIOG, Part II, 12-6.)  
(Formerly 12-2.1.2) |

(1) SAs must be armed at all times when on official duty with the handgun secured to the Agent's person in an approved holster. Immediate access to the handgun and security are paramount. Briefcases, handbags, etc., are not generally acceptable methods of carrying a firearm. Loss of or damage to a weapon related to nonholster storage or the inability to access a weapon when necessary may result in recommendation for administrative action.

SAs are authorized to be armed when off-duty.

(2) The SAC or designee is ultimately responsible for assignments where firearms might be used. The SAC should be on-scene if possible.

(3) Safety levers should not be engaged on any pistol constructed with a double action first shot (e.g., Smith & Wesson 459, 659, 3913). With the exception of single-action pistols (e.g., Browning Hi-Power), handguns should not be holstered in a cocked mode.

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 6

(4) When an SA is moving with a drawn weapon, the finger must be off the trigger; double-action weapons should be decocked; the manual safety should be engaged on single-action weapons. Safety is the paramount consideration. Unless obvious and articulable circumstances dictate otherwise, these safety rules should NOT be violated.

(5) To preclude unintentional discharges when covering an adversary, double-action weapons should be decocked and finger off the trigger. Single-action weapons (including shoulder weapons) should have the safety engaged and finger off the trigger.

(6) When SAs are armed, handguns must be fully loaded.

(7) Unless operationally deployed, shoulder weapons should be maintained with an empty chamber. Prior to entry into areas where potential danger exists, a round should be chambered in all shoulder weapons. The safety should remain engaged until the circumstances require placing the weapon in the "fire" mode.

(8) SAs must be familiar with and currently qualified with all firearms and equipment they carry.

(9) When possible, emphasis must be placed on planning arrests to ensure superiority of manpower and firepower to exert maximum pressure on the individual(s) being sought, thereby reducing the opportunity for a subject to resist or flee.

(10) SAs may draw their weapons without being confronted with a deadly force situation. Proper training, good judgment and experience in arrest situations must be relied upon to provide the proper response when confronted with potential deadly force situations.

(11) SAs should avoid unreasonable display of weapons in public.

(12) Accidental or unintentional discharge of a weapon is extremely dangerous to the public and to FBI personnel. Avoid unnecessary handling of weapons and never dry fire weapons unless on a range or other safe, suitable area. ANY unintentional discharge must be reported to FBIHQ using FD-418.

(13) Specialized weapons, i.e., M16, MP5, gas delivery systems, etc., must only be deployed by SAs trained and currently qualified in their use.



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 7

EFFECTIVE: 04/07/97

|12-2.3| Firearms Aboard Aircraft (See MIOG, Part I, 164-15 (4).)  
|(Formerly 12-12.1.3)|

(1) Title 49, USC, |Chapter 465, |Section 46505, generally  
forbids carrying firearms aboard aircraft. |FBI Special Agents| are  
exempt from this prohibition.

(2) FAA Federal Air Regulation 108.11 (a) (Title 14, CFR,  
Section 108.11) recognizes the authority of FBI SAs to carry firearms  
aboard aircraft at all times.

| (3) | The FBI has exclusive jurisdiction over the Aircraft  
Piracy Statute, Interference with Flight Crew and certain crimes  
aboard aircraft.

| (4) | FBI SAs |MUST| carry a firearm ON THEIR PERSON aboard  
any commercial domestic flight when on official business, unless  
operational considerations dictate otherwise. |Firearms may NOT be  
carried in a purse, briefcase or carry-on luggage. Under no  
circumstances should an Agent surrender their weapon to airline  
personnel. |

(5) |Agents are encouraged, but not required, to carry  
their firearm when traveling aboard a commercial airline when  
traveling within the United States for reasons other than official  
duty. If carried, the firearm MUST remain on the Agent's person.

(6) FBI SAs must complete the appropriate airline forms  
for traveling while armed and comply with airline and airport  
procedures.

(7) FBI SAs are prohibited from consuming alcoholic  
beverages while traveling armed on aircraft or within eight hours of  
travel.

| (8) | SAs must avoid unnecessary display of |firearms while|  
traveling by aircraft.

| (9) | The aforementioned FAA Regulations apply to U.S. flag

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 8

carriers operating between points within the United States and its Territories. When official duty involves travel through or to a foreign country, the traveling Agent must determine beforehand the laws of the country being visited or transited regarding firearms, and prior approval to carry a firearm in that country must be obtained.

(10) If operational or travel considerations do not permit the carrying of a firearm, firearms may be placed in checked baggage for retrieval at the destination. Firearms placed in checked baggage must be unloaded and secured in a hard side, locked case. The weapon must be declared to the ticket agent at the time of check-in and the airline "firearm" tag placed ~~INSIDE the locked suitcase.~~

EFFECTIVE: 04/07/97

12-3 ISSUED WEAPONS

(1) FBI SAs are authorized to carry and utilize only issued or Bureau-approved personally owned weapons (POWs) regardless of on- or off-duty status.

(2) Any firearm, regardless of Bureau-issued or personally owned status is referred to as ASSIGNED PROPERTY.

(3) Firearms can only be carried by those Bureau employees who are (1) authorized to use firearms in connection with their official duties and (2) are currently qualified.

(4) All Bureau handguns should be sighted in for accuracy during firearms sessions

b2  
b7E

(5) Any changes or alterations to any assigned weapon must be authorized by the Firearms Training Unit and must be accomplished by the FBI Gun Vault at Quantico. Exceptions to this requirement must be requested in writing and approved by the Gun Vault.

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 9

EFFECTIVE: 04/07/97

12-3.1 Distribution of Firearms

| Each field office should maintain an adequate number of handguns and shoulder-fired weapons available for issue as needed. |

(1) Handguns -

(a) SAs are issued a handgun and associated holster and ammunition or magazine pouches while attending New Agents Training. This weapon will generally remain assigned to the Agent throughout his/her career. Exceptions may result due to loss or damage of the weapon or replacement of the weapon at the direction of the Firearms Training Unit (FTU).

(b) Handguns are intended for general self-defense and should not be exclusively relied upon for planned offensive operations such as the execution of search warrants or arrests where shoulder-fired weapons may be more appropriate. |

(c) | Small-framed handguns (i.e., Smith and Wesson revolver Models 36, 49, 60; Glock 26 and 27 pistols, etc.) are most useful when concealability is important and should not be considered as a primary firearm in most situations. |

(2) Shotguns

| Shotguns should be issued on an extended basis to Agents assigned to investigations/duties where contact with armed subjects is likely (i.e., drugs, Violent Crimes and Major Offenders, resident Agents, [REDACTED] etc.). Shotguns from the division gun vault may also be issued for short terms on an as-needed basis (i.e., warrant executions). |

b2  
b7E

(3) Rifles

(a) | Sniper rifles and rifles capable of fully automatic fire are authorized for use only by current firearms instructors [REDACTED] who are qualified in the weapon's use. Any exception to this requirement must be requested in writing and approved by the Unit Chief, FTU. |

b2  
b7E

(b) | Any SA qualified in the use of a rifle may use a

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 10

rifle capable of automatic fire if it is equipped with a fire selector lock to prevent fully automatic fire.

(c) The SAC or designee may authorize the removal of the selector locks during emergency situations. This authority may not be delegated. Upon termination of the emergency situation the SAC must ensure the selector locks are properly reattached to the weapons.

(d) Bureau rifles should be sighted in during firearms training sessions to ensure accuracy at operationally appropriate distances.

(4) Submachine Guns

(a) The Bureau is generally equipped with Heckler and Koch (H&K) submachine guns.

(b) Submachine guns may only be used operationally by current firearms instructors, [REDACTED] currently qualified in their use. The MP5-10/A2 which is capable of a two-shot burst may be utilized by any Agent who is currently qualified on that weapon.

b2  
b7E

(c) The Thompson submachine gun may only be used for display and demonstration purposes.

(5) Carbines

(a) The Bureau is equipped with Heckler and Koch (H&K) and Colt carbines.

(b) All SAs are authorized to use the H&K MP5SF and Colt M16 series of carbines, provided they are currently qualified with the weapon. The weapon must be equipped with a fire control selector lock if capable of fully automatic fire.

EFFECTIVE: 04/07/97

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 11

12-4 PERSONALLY OWNED WEAPONS

(1) SAs are authorized to carry approved personally owned weapons (POWs) in lieu of a Bureau-issued firearm, provided the SAs are currently qualified with those weapons.

(2) SAs are authorized up to two POW handguns in addition to a Bureau-issued pistol or revolver. Agents may elect to have three POW handguns but the Bureau-issued handgun must be returned to the FBI Academy Gun Vault and the Bureau-issued gun removed from the SA's property record. POW handguns authorized for duty may be any combination of pistols and/or revolvers.

(3) SAs are authorized one POW 12-gauge shotgun with a barrel length between 18 and 20 inches and fixed stock, provided the SA is qualified with that weapon.

(5) The Firearms Training Unit (FTU) and FBI Academy Gun Vault maintain an up-to-date list of firearms approved for official use as well as accessories authorized for these firearms. Additionally, the FTU will provide the list of approved handguns, shotguns and rifles/carbines with approved accessories to the field division PFIs in the Annual Field Firearms Program communication. Agents should consult with the PFI or the FTU BEFORE purchasing a firearm for official use.

(6) Before approval of a POW is granted, the weapon must be inspected by the FBI Academy Gun Vault for functional reliability, accuracy and serviceability.

(7) Approval for POWs will only be granted for currently manufactured models. Once a weapon is discontinued by a manufacturer, that model will no longer be approved. Previously approved weapons in this category will continue to be approved until removed by submission of FD-431. Likewise, once a weapon no longer approved is removed from an Agent's FD-431, that weapon will not be approved for official use by another Agent.

(8) POWs authorized to be carried on official business are to be treated in the same manner as nonexpendable Bureau property.

(9) No POW will be approved for use which requires an application for National Firearms Act (NFA) approval from the Bureau of Alcohol, Tobacco and Firearms (ATF). Those weapons that apply as listed in Title 18, Section 5845 are as follows:

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 12

- (a) A shotgun having a barrel or barrels of less than 18 inches in length;
- (b) A rifle having a barrel or barrels of less than 16 inches in length;
- (c) Any weapon mentioned in (a) or (b) above which has an overall length of less than 26 inches;
- (d) Any machine gun (fully automatic weapon);
- (e) Any silencer or suppressed weapon.

(10) POWs must have a factory finish from the manufacturer. The Gun Vault will be responsible for blued or parkerized finishes only. If the condition of the finish renders the weapon unserviceable, authority to carry that weapon may be withdrawn. Refinishing other than bluing or parkerizing must be completed by the manufacturer at the Agent's own expense.

(11) Approval Procedure

(a) The field division PFI will manage this program for the office.

(b) An SA seeking weapon approval will submit an FD-431 in quadruplicate to PFI with the weapon for inspection and initial approval.

(c) The PFI (or a designated firearms instructor) will verify that the weapon meets the requirements for a POW in terms of condition, serviceability, required features, and being an approved model.

(d) The PFI (or a designated firearms instructor), after signing the FD-431, will submit the forms for SAC approval and transmittal, returning three copies of the FD-431 to the FBI Academy Gun Vault WITH THE WEAPON. The submitted FD-431 MUST contain the PFI's signature and SAC or designee's initials. One copy of the FD-431 should be maintained as a field office tickler copy. Pistols must be accompanied by four factory magazines. Rifles must be submitted with a minimum of two factory magazines.

(e) The aforementioned approval process may be modified when an Agent purchases an approved firearm directly from a manufacturer who will ship the weapon directly to the FBI Academy Gun

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 13

Vault. The FD-431 is completed by the requesting Agent, approved by the PFI and SAC, and three copies forwarded to the FBI Academy Gun Vault. The FD-431 will then be matched with the gun received from the manufacturer.

(f) Weapons must be clean, unloaded, properly packaged, and properly shipped.

(g) The Gun Vault will inspect the firearm for physical condition and test fire the weapon for functional integrity.

(h) If the weapon meets all necessary inspection prerequisites, the firearm will be returned to the submitting PFI with the FD-431 marked "approved." The Bureau will not supply parts needed to make a weapon acceptable for approval.

(i) SAs must fire a qualifying score on the current qualification course for the weapon in question and appropriately record scores BEFORE authority to carry the weapon will be granted by the PFI.

(j) Once the approval procedure is complete, the SA is authorized to carry this POW. The approval copy of FD-431 should be placed in the SA's personnel file.

(k) Any reason for disapproval of a weapon will be explained in full on the FD-431 which will be returned with the weapon to the submitting PFI.

(12) To remove a POW from Bureau-approved status, properly execute Form FD-431 in quadruplicate and forward three copies to Quantico. Upon receipt of the return copy from Quantico, the PFI will delete this weapon from the Agent's firearms training records.

(13) No firearm is authorized for official use unless it is physically inspected and authorized by the Gun Vault (i.e., seized weapons, personal purchases, etc.).

EFFECTIVE: 04/07/97

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 14

12-4.1 | Revised and Moved to 12-4 |

EFFECTIVE: 04/07/97

12-5 MAINTENANCE AND REPAIRS

(1) SAs are personally responsible for security and maintenance of all firearms and other expendable and nonexpendable related equipment assigned to them.

(2) Alterations, repairs, and refinishing of assigned firearms must be conducted by FBI gunsmiths. Exceptions include refinishing by manufacturers or other contractors whose use has been requested in writing and approved by the Firearms Training Unit (FTU) in advance.

(3) After-market parts or options will not be approved unless authority is requested in writing and approved by the FTU Unit Chief. Questions regarding the installation of after-market parts on a Bureau-approved firearm should be resolved PRIOR to purchase of these parts or modifications by contacting the FTU.

(4) SAs are to bring all Bureau-assigned handguns to the Gun Vault for preventive maintenance, inspection and repair each time they attend an in-service or conference at the FBI Academy.

(5) Firearms must be unloaded, cleaned, and properly packaged before shipment via Federal Express, or other appropriate means. When returning a firearm to the FBI Academy Gun Vault for service or turn-in, a cover communication should be included which states the reason the firearm is being returned. Firearms being returned should be addressed: FBI Academy, Room 110, Building DN, Quantico, Virginia 22135. (DO NOT MAIL WEAPONS ADDRESSED "ATTENTION: GUN VAULT.") (See MAOP, Part I, 17-1.7.1; Part II, 2-2.2.2, 6-2.3.9, and 6-10.2.)

(6) When it becomes necessary to render a weapon inoperable during the course of an investigation, this procedure must be accomplished by an FBI gunsmith.

(7) Field offices intending to use seized guns for



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 15

demonstrations or teaching purposes must first submit those weapons to the Gun Vault for inspection, approval, and possible modifications to render them safe.

EFFECTIVE: 04/07/97

12-5.1 Care of Firearms

(1) After being used, and periodically during storage, all weapons should be carefully cleaned and lubricated per the manufacturer's recommendations. Care should be taken to prevent excess solvent and oil from entering inaccessible areas of the firearm.

(2) Excess oil and solvent must be completely wiped off wood stocks. Do not allow any oil or solvent to come in contact with the lenses of any telescopic sights or night sights.

(3) Due to the fact that handguns are almost continually encased in leather holsters, regular inspection and lubrication should be conducted to prevent rusting.

(4) Questions pertaining to the care, cleaning and maintenance of firearms should be addressed to the PFI or FBI Academy gunsmiths.

EFFECTIVE: 04/07/97

12-5.2 Deleted

EFFECTIVE: 04/07/97

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 16

12-6 SECURITY OF WEAPONS | (See also MIOG, Part II, 12-2.2.) |

(1) Each SA is personally responsible for the security of weapons under his/her control.

(2) SACs must provide |secure| storage areas for Bureau-assigned firearms in Bureau office space.

(3) When on duty and out of the office, handguns should be kept on the SA's person unless operational considerations or good judgment dictate otherwise.

(4)  b2, b7E

(5) When SAs remove handguns from their person, it is recommended that the weapon and holster be removed together to prevent unintentional discharge. |This recommended action is made to minimize unnecessary unloading/loading of weapons within Bureau office space. |

(6)  b2, b7E

(7) All firearms stored in Bureau office vaults or other approved areas must be unloaded, functional and clean.

(8) All operational shoulder weapons, whenever possible, should be stored muzzle end down to facilitate the natural movement of lubricants toward the barrel end.

(9) All weapons should be stored UNLOADED in the following manner:

(a) Revolvers - cylinder closed, hammer down.

(b) Pistols - |magazine removed, slide closed, hammer released and chamber plug inserted if available. |

(c) Remington Model 870 shotgun - action closed, trigger snapped, safety on.

(d) Colt Model |M16/AR-15 series of |rifles or carbines - magazine removed, action closed, trigger snapped, fire selector on "SEMI."

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 17

(e) Winchester/Remington rifles - action closed, trigger snapped, safety off.

(f) Thompson submachine gun - magazine removed, action closed, fire selector on "SINGLE," safety on "FIRE."

(g) H&K MP5 (all models) - magazine removed, action closed, trigger snapped, safety on.

(h) M79 Grenade Launcher - action closed, trigger snapped, safety on.

(i) Federal Gas Gun - action closed.

EFFECTIVE: 04/07/97

12-6.1 Security of Weapons at Residence or Nongovernment Space

(1) SAs are personally responsible for security of all assigned firearms to prevent unauthorized handling or unintentional discharge.

(2) When devices or containers are provided by the Bureau for the storage of weapons away from Bureau space, SAs should make use of this equipment whenever possible.

(3) When unattended, each firearm must be made inoperable by one or more of the following methods:

(a) Remove and separate the source of ammunition.

(b) Install commercially available pistol lock, trigger lock, or cable lock.

(c) Contain in a commercially available lock box or other container which will provide appropriate security.

(4) Bureau personnel authorized to carry a firearm must use the utmost caution when storing and securing their firearm at home when children are present. In addition to great personal grief, many states have laws providing for severe criminal and civil penalties when anyone is injured or killed as a result of a child

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 18

obtaining access to a firearm. Bureau employees are to ensure the security and storage of their firearm(s) complies with pertinent state and local laws.

EFFECTIVE: 04/07/97

12-6.2 Vehicles (See MAOP, Part I, 1-3.2.)

(1) No Bureau-assigned firearm may be left in the passenger compartment of an unattended Bureau vehicle or vehicle authorized for official use unless the vehicle doors are locked and the firearm is secured in a locked vehicle weapons mount or other secure device or container which cannot be readily removed from the vehicle, and circumstances prevent more secure storage.

(2) [REDACTED] Even when properly secured, firearms should not be left in unattended vehicles overnight unless required by operational circumstances.

b2 b7E

(3) Other nonexpendable Bureau equipment related to Agent safety may be maintained in the passenger compartment of an unattended Bureau vehicle or vehicle authorized for official use for short periods of time only if required by operational necessity or good judgment, and only if properly concealed and with the vehicle doors locked. "Properly concealed" means placed in an appropriate container and/or secreted within the vehicle to prevent observation and identification of the item from the vehicle exterior.

(4) Any nonexpendable Bureau equipment not related to SA safety should be maintained in the locked trunk of an unattended Bureau vehicle or vehicle authorized for official use, but should not be left overnight unless operational circumstances dictate otherwise.

(5) [REDACTED]

(6) [REDACTED]

b2 b7E

(7) [REDACTED]

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 19

b2  
b7E

(8) The standards set forth above are MINIMUM standards. Employees are expected to exercise good judgment in providing adequate security to all such equipment and firearms. Personal inconvenience is not considered an adequate reason for deviation from these minimum standards.

(9) Reports of lost/stolen firearms related Bureau property should be submitted to the Firearms Training Unit AND the Adjudication Unit, Office of Professional Responsibility, for replacement and possible administrative action.

EFFECTIVE: 04/07/97

12-7 AMMUNITION

(1) SAs and other Bureau employees authorized to carry firearms may load their Bureau-assigned weapon(s) only with ammunition provided or approved by the FBI.

(2) It is the SAC's responsibility to ensure that the field office maintains an adequate supply of ammunition for training and operational contingencies.

(3) Field office ammunition inventories should be rotated to promote serviceability and be inspected a minimum of once each quarter.

(4) All ammunition should be stored in a secure, and preferably dehumidified, controlled temperature environment.

(5) During training, any ammunition authorized for FBI use may be fired. At all other times outside of training sessions, FBI authorized service ammunition must be used.

(6) Ammunition carried on the person should be used during the next firearms training session and replaced with a fresh supply.

(7) 9 mm 124 grain ball "training" ammunition may be used

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 20

operationally in the suppressed MP5 SD only. This round is limited to training use only in all other Bureau-issued/approved 9 mm weapons.

(8) The Firearms Training Unit is the procurement point for all ammunition used by Bureau personnel for official purposes.

EFFECTIVE: 04/07/97

12-7.1 Deleted

EFFECTIVE: 04/07/97

#### 12-8 FIREARMS PROCUREMENT

(1) The acquisition of firearms as Bureau property must be (1) approved by the FTU, and (2) administered by the FBI Academy Gun Vault.

(2) All firearms purchased or obtained by a field office as Bureau property must be shipped directly to the FBI Academy Gun Vault for inspection and test firing before use.

(3) Any exceptions to this policy must first be requested in writing and approved by the FTU before procurement.

EFFECTIVE: 04/07/97

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 21

12-9 FIREARMS IN RESIDENT AGENCIES

(1) Firearms may be maintained in resident agencies.

(2) All handguns and shoulder fired weapons should be stored in a secure safe, vault or safe-type cabinet. Reasonable security precautions such as weapons locked and stored in locked cabinets or closets within alarmed Bureau space may suffice in lieu of storage in a safe.

(3) Field offices are authorized to purchase safes, vaults, or safe-type cabinets in order to provide secure storage of firearms.

(4) All other policies cited herein that govern the use and maintenance of Bureau-assigned firearms and ammunition also apply.

(5) Any exceptions to this policy must be requested in writing and approved by the FTU.

EFFECTIVE: 04/07/97

12-10 FIREARMS TRAINING

(1) Firearms training requirements are submitted to the field annually by EC to all SACs, captioned, "Field Firearms Training Program."

(2) The objective of the FBI firearms training program is to provide four MANDATORY qualification sessions annually. Since firearms training is a perishable skill, however, the FTU encourages field offices to provide additional training opportunities. Field offices whose range availability and ammunition supply will not support mandated training should submit a proposed training plan to the Training Division, FTU, for approval. This plan should include the number of sessions, courses to be used, and the number of rounds to be fired.

(3) The SAC is ultimately responsible for all firearms training, weapons and ammunition inventories, and execution of the Field Firearms Program.

(4) SAs and all other personnel authorized to carry

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 22

firearms must meet or exceed the minimum proficiency and safety standards set forth in the Annual Field Firearms Program.

(5) PFIs are responsible for all transition training either from revolver to pistol or pistol to revolver. The PFI must be satisfied that an SA has successfully completed the requirements of transition training and proficiency checklist as specified in training curricula provided by the FTU and is qualified to carry that weapon. The PFI must verify this training by documentation on or attached to the SA's FD-40.

(6) Each PFI should adhere to the format of the calendar year Field Firearms Program provided by the FTU. Any changes must be submitted via written communication and approved in advance by the Unit Chief, FTU.

(7) All firearms training sessions must be supervised by the PFI or a Bureau-certified firearms instructor designated by the PFI.

(8) All SAs are required to attend defensive tactics training conducted in conjunction with each of the firearms qualification sessions.

(9) The Defensive Tactics Training Course will be managed by the Principal Defensive Tactics Instructor in each field division. This program is submitted to each office as part of the annual Field Firearms Training Program.

(10) Field offices must report the following by electronic communication captioned, "Annual Field Firearms Training Report," to the FTU by close of business 12/31:

(a) Dates of training sessions

(b) Ranges utilized

(c) Names of instructors assisting each session.

These names should also be listed at the bottom of FD-39 score cards.

(d) Names of Bureau personnel who have missed ANY mandatory training sessions, with the reason for each delinquency specified. ALL delinquencies must be reported.

(e) Names of all Bureau personnel who have failed to shoot qualifying scores with any authorized weapon. Include date last



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 23

qualified.

(11) The PFI is to ensure that ranges used for field firearms training are inspected and contain no safety hazards that would endanger FBI personnel or others.

(12) PFIs are to make every effort to ensure that the air quality of indoor ranges used for training complies with the Occupational Safety and Health Administration (OSHA) standards. A certificate of compliance with these standards should be available for review at the range facility. If an indoor range does not comply with OSHA standards, this facility should not be used for training.

(13) The authority in charge of a particular range should be advised of any safety deficiencies noted.

EFFECTIVE: 04/07/97

12-10.1 Firearms Delinquencies

(1) Any employee authorized to carry firearms who does not attend firearms training during a firearms training period is considered delinquent. To ensure compliance with this requirement, the SAC (or AD in the case of FBIHQ) may, at their discretion, require delinquent individuals to surrender their firearms and make any necessary recommendations to the Adjudication Unit, Office of Professional Responsibility (OPR), FBIHQ, for administrative action if appropriate. The individual's authority to carry a firearm is rescinded and the weapon should only be issued for training purposes until the delinquency is corrected. No SA should be permitted to become delinquent for any firearms training period unless documented medical circumstances dictate otherwise AND the SA has been placed on medical mandate by FBIHQ Health Care Programs Unit. The FTU is to be advised of each delinquency in the "Annual Field Firearms Training Report."

(2) Those Agents who were unable to attend firearms training on their regularly scheduled days should be rescheduled at the earliest convenience during the training period. Delinquencies must be corrected as soon as possible.

(3) Whenever authority to carry a weapon is rescinded, a memorandum of explanation should be attached to the SA's FD-40.

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 24

EFFECTIVE: 04/07/97

12-10.2 Firearms Qualification

EFFECTIVE: 05/20/94

12-10.2.1 Firearms Qualification Policy (See MIOG, Part II,  
12-10.4; MAOP, Part I, 20-28.3.)

(1) SAs must qualify with ALL weapons they are authorized to carry.

(2) SAs must qualify a minimum of four times per calendar year.

(3) SAs must qualify with each assigned handgun a minimum of once per year. It is recommended that weapons regularly carried on duty be fired for qualification at each firearms session.

(4) Specific training requirements are set out in the Field Firearms Training Program submitted by the FTU for each calendar year. PFIs are required to follow current established course protocols set by the FTU.

(5) Agents will qualify within their assigned division. Agents assigned to FBIHQ, the Engineering Research Facility, and the FBI Academy will qualify with the FTU at Quantico.

Exceptions:

(a) Agents assigned on a temporary duty basis to another division which would preclude their qualification in their assigned division, may qualify with the host division. It is the responsibility of the PFI in the host division to ensure the TDY

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 25

Agent's scores are recorded and forwarded to the PFI of the Agent's assigned division.

(b) Agents wishing to qualify with another division for convenience must have the concurrence of the PFI from their assigned division and the host division. The PFI of the host division must record the visiting Agent's scores and forward these to the PFI of the Agent's assigned division.

(c) Agents assigned to FBIHQ, the Engineering Research Facility and the FBI Academy wishing to qualify with another division must have the concurrence of the FTU and host PFI. The PFI of the host division is responsible to ensure the visiting Agent's scores are recorded and reported to the FTU.

EFFECTIVE: 04/07/97

12-10.2.2 Recording Firearms Scores

(1) The names of SAs receiving firearms training should be indicated on the Form FD-39 or an approved automated system.

(2) The individual scores shall be entered in the appropriate column of Form FD-39. This form shall contain the names of all SAs attending firearms training and the make and model of issue/approved firearm(s) used for qualification. Supervising firearms instructors shall be listed at the bottom of FD-39.

(3) After completion of a training period, scores are to be transferred from the FD-39 to each SA's FD-40 or automated form. FD-39s are retained for one year, then destroyed; FD-40 is a permanent record and must accompany the SA's personnel file upon transfer.

(4) The PFI or designated firearms instructor will score the targets on qualifying courses.

EFFECTIVE: 04/07/97

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 26

12-10.2.3 Failure to Qualify

(1) If an SA fails to qualify, the PFI must provide remedial training and an opportunity to qualify on the next regularly scheduled qualification day.

(2) After opportunities have been provided for qualification and failures continue to exist, the PFI must advise the FTU in the Annual Field Firearms Training Report.

(3) Employees must demonstrate proficiency to be permitted to carry firearms. If the employee cannot qualify after remedial training on two out of three qualification attempts, the SAC must require the employee to surrender his/her firearm. The Agent will be issued his/her weapon only for training until such a time as a qualifying score is shot. When an Agent's authority to carry a firearm is rescinded, this action must be noted on the Agent's FD-40.

(4) Chronic unexcused delinquency or failure to qualify should be reported to the FTU and Adjudication Unit, Office of Professional Responsibility, with recommendations for administrative action, if appropriate.

EFFECTIVE: 04/07/97

12-10.2.4 Shoulder Weapons - Qualification

SAs will qualify with each assigned shoulder weapon at least twice per year. Agents are encouraged to train with weapons they regularly carry at EVERY training session. SAs with an assigned shoulder weapon will use that specific weapon when qualifying. Agents not assigned a specific shoulder weapon will, at a minimum, demonstrate proficiency with the shotgun and MP5 at least once per year as specified in the Annual Field Firearms Program.

EFFECTIVE: 04/07/97

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 27

12-10.3 Firearms Safety Rules

(1) Cardinal Rules:

(a) Treat all firearms as if they are loaded.

(b) Never point a weapon at anyone unless you are justified in doing so.

(c) Keep your finger off the trigger unless you intend to shoot.

(2) General Rules:

(a) All live-fire FBI firearms training must be supervised by an FBI Firearms Instructor.

(b) When transporting weapons on your person to and from the range, handguns should be holstered; shoulder weapons should be in a safe condition and carried with the muzzle pointed straight up.

(c) Safety precautions must be adhered to and enforced. Discipline must be maintained. Unsafe and careless behavior will not be tolerated, should be reported, and may result in recommendations for administrative action.

(d) Immediately upon picking up a firearm, face a safe direction, activate the safety if present, remove any ammunition, open the action and check to see that the weapon is unloaded. Check it again.

(e) Never give to or receive a firearm from anyone, unless the weapon is unloaded and the action is open allowing the person receiving the weapon to see that it is unloaded. Always present the weapon BUTT first.

(f) Never anticipate a command. Avoid unnecessary conversation, and pay attention to instructors. You will be told exactly what to do.

(g) Perform a safety check on the weapon before a training session. Make sure the weapon is unloaded. After training, you also need to ensure the weapon is unloaded before cleaning.

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 28

(h) Load and unload only on the firing line and only when instructed to do so. Any exceptions will be stipulated by the lead Firearms Instructor.

(i) Keep the firearm pointed down range or in a safe direction at all times and ALWAYS be aware of potential dangers in any direction your weapon may be pointed.

(j) Use only one hand when holstering a handgun. Any exception will be so stipulated by the lead Firearms Instructor.

(k) No smoking, eating or drinking on the firing line because of health risks associated with lead residue.

(l) Never permit the muzzle of a firearm to touch the ground.

(m) In case of a misfire or malfunction, perform an immediate action drill, unless instructed to do otherwise.

(n) After firing a shot that does not sound as loud as it should, clear the weapon and check to see if a bullet is lodged in the barrel.

(o) Never leave your firing position unless instructed to do so.

(p) Never remove a weapon from the holster in training, unless instructed to do so.

(q) Never dry fire on the range unless under direct supervision of a Firearms Instructor. Exceptions will be specifically identified by the lead Firearms Instructor.

(r) Eye and ear protection are mandatory when firing on the range. Ear plugs should be worn ONLY IN CONJUNCTION with proper sound barriers and are NOT a substitute for issued or equivalent hearing protection.

(s) Everyone is responsible for range safety. Immediately report any safety violations you see to a Firearms Instructor.

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 29

EFFECTIVE: 04/07/97

12-10.4 Firearms Training of Non-Agent Employees

As a rule, only Agents receive firearms training from the Bureau. Exceptions are:

(1) Electronics technicians and security patrol clerks specifically authorized by FBIHQ.

(2) Uniformed Police Officers of the FBI.

(3) Other non-Agent personnel with special authority to carry firearms (e.g., Special Deputy U.S. Marshal).

(4) Non-Agent personnel authorized to carry firearms must:

(a) be approved by their SAC or Section Chief

(b) comply with deputation requirements established by the USMS, and

(c) be engaged in official activities for which the carrying of a firearm has been authorized.

(5) All non-Agent personnel who are authorized to carry firearms will comply with all regulations in this section that normally apply to SAs (see MIOG, Part II, 12-10.2.1). In addition, they must also attend annual legal training, quarterly defensive tactics training, and participate in the Fitness Indicator Test (FIT).

EFFECTIVE: 04/07/97

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 30

12-10.5 Police Firearms Training

(1) FBI firearms instructors may conduct police firearms schools.

(2) Firearms training is to be given only to law enforcement groups unless an exception is authorized by the SAC (e.g., safety training for Bureau employees and their family).

(3) The primary firearms instructor must ensure that ranges used for firearms training are inspected and contain no safety hazards that would endanger FBI or police personnel.

EFFECTIVE: 04/07/97

12-10.6 Firearms Instructors Policy (Formerly 12-10.6.1)

(1) To qualify as a Bureau firearms instructor, candidates must attend the Firearms Instructor In-Service (FAIS) presented by the FTU.

(2) To maintain instructor status, employees must qualify quarterly and obtain the following minimum scores when these courses are fired:

- (a) 30 round bulls-eye course
  - 1. One-hand score 240, or
  - 2. Two-hand (optional) score 260

(b) Double Action Course score 90

(c) PQC score 90

(d) Shotgun 10A score 90

(e) MP5 (qualification course) score 90

(3) To maintain instructor status, in addition to shooting instructor level scores on courses listed in (2) above, each instructor must participate in at least one documented Bureau firearms



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 31

training session per year.

(4) Firearms instructors must attend a Recertification Program with the FTU at least once every four years. Agents transferring out of the FTU are considered recertified for a period of four years.

(5) Failure to comply with instructor requirements will result in the loss of current status. The employee will be listed officially as firearms instructor - inactive.

(6) To regain active firearms instructor status, the employee must attend a Recertification Program at the FBI Academy and demonstrate proficiency as noted in (2) above.

EFFECTIVE: 07/17/97

| 12-10.6.1 | Revised and Moved to 12-10.6 |

EFFECTIVE: 04/07/97

| 12-10.7 | Target Guidelines |

| (1) | STEEL TARGET POLICY

| (a) - Standard | service and training ammunition | may not be used on steel targets | at distances less than ten yards. Some types of frangible ammunition may | be used on | steel targets at closer distances.

| (b) | To minimize | potential injury from | ricochets, firing positions should be perpendicular to the target line.

| (c) | Construction of any steel targets MUST be coordinated through the | FTU to ensure targets meet minimum hardness and safety standards.

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 32

(d) PFIs are responsible for permitting only the use of proper weapons and ammunition on steel targets to prevent damage or destruction to the target, reduce ricochet and prevent injury to personnel.

(e) Steel targets must be inspected before each training session.

(f) All personnel on the steel course site must stand behind the shooter. In multiple courses, the shooter must not be ahead of another shooter.

(g) All personnel on the steel course site must continuously wear eye and ear protection. Personnel on a steel course should also wear issued body armor.

(h) Damaged targets, i.e., dimpled, punctured, or bowed, are unsafe and should not be used.

EFFECTIVE: 04/07/97

12-11 SHOOTING INCIDENTS (See MAOP, Part II, 8-1.3.2.)

EFFECTIVE: 10/17/95

12-11.1 Reporting of Shootings (See MIOG, Part II, 12-11.8; MAOP, Part II, 8-1.3.2.)

(1) In all shooting incidents involving the intentional use of force by FBI personnel and in all incidents, intentional or otherwise, WHERE INJURY OCCURS, notify the Violent Crimes and Major Offenders Section (VCMOS) Chief, CID, FBIHQ by telephone, followed by teletype. Similarly, in all shooting incidents occurring in joint investigations or FBI led/controlled task forces where a non-FBI participant fires a weapon, notify the VCMOS, CID, FBIHQ by telephone, followed by an airtel within seven days.

(2) Other instances involving the discharge of a firearm

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 33

| by FBI personnel | must be reported as soon as time permits by teletype to the Chairperson, Shooting Incident Review Group (SIRG), with a copy to the Firearms Training Unit (FTU). FD-418 (Shooting Incident Report), in triplicate, is to be submitted to the FTU by airtel within five working days. SA's FD-40 (Firearms Record) should be attached to the FD-418.

(3) | If an FBI employee is injured, designate one copy of teletype for the Office of | Public | and | Congressional Affairs. |

(4) SAC must personally ensure that investigations | related | to Agent-involved shooting incidents are handled quickly and properly.

(5) | If the SAC or ASAC was involved in the planning or execution of events, FBIHQ should be advised during initial contact. |

(6) | Initial teletype should include the SAC's recommendation whether the shooting inquiry should be conducted by the field division under the direction of the SAC, or by a Shooting Incident Response Team (SIRT) under the direction of an Inspector or Inspector-in-Place (IIP). Generally, this determination is based on the extent of SAC or ASAC participation in the planning and operational events of the incident. |

(7) | The Assistant Director, Inspection Division (INSD), in consultation with the SAC and Assistant Director, CID, will make the determination whether a shooting inquiry will be conducted under the direction of the SAC or an Inspector/IIP. |

(8) | If an Inspector/IIP is not dispatched to the scene, the SAC will advise and confirm by teletype that he/she is directing the necessary required shooting inquiry investigation, UACB. |

(9) | A shooting inquiry must be conducted under the direction of the SAC when a weapon is discharged by FBI personnel unless circumstances necessitate the inquiry be conducted under the direction of an Inspector/IIP. |

(10) | In joint or task force investigations wherein a local, state, or other federal law enforcement officer fires a weapon or is shot, but no shots are fired by FBI personnel who are present:

(a) Joint investigation - SAC or ASAC will notify FBIHQ by telephone, followed by an airtel delineating the following:

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 34

1. Activities of accompanying officer and circumstances which led to the shooting.
2. Details of raid/arrest plan.
3. Instructions given to accompanying officer.
4. Results of local shooting inquiry conducted, if available; records of interview(s), and analysis.

(b) FBI led/controlled task force:

1. Include all of (a) above, plus:
  - a. Degree of FBI supervision exercised over the officer's day-to-day investigative activities (generally reflected in implementing Memorandum of Understanding (MOU)).
  - b. Chain of command within the task force.
  - c. A copy of any MOU delineating task force responsibilities of non-FBI personnel.

(c) Submit within seven days, an original and 12 copies of the shooting incident airtel to the Assistant Director, INSD, Rm. 7129, Attention: SIRG, with one copy designated to the FTU.

(11) through (22) Moved to MIOG, Part II, 12-11.7, 12-11.8, and 12-11.9.

EFFECTIVE: 10/17/95

12-11.2 Guidelines for Intervention at the Shooting Scene (See MAOP, Part II, 8-1.3.2.)

(1) After the shooting scene has been secured, the first concern expressed and acted upon will be that all Bureau personnel are well cared for both physically and mentally.

(2) The Agent(s) involved in the shooting incident will be permitted and encouraged to immediately contact his/her spouse

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 35

and/or family. If the Agent has been injured, or if he/she feels it would be useful, the Agent's family will be contacted immediately in person by a designated Agent who knows the family personally. The field office will also be notified of the Agent's condition so that there will be a response to the family who called the office. It is particularly important that family notification occur before press and/or media accounts appear.

(3) Agents who have been personally involved in the shooting incident will be removed from the scene as soon as possible and not assigned further duties in the investigation of that incident.

(4) If the Agent's weapon is secured for evidence or ballistics tests, another will be issued immediately unless there is cause not to issue a weapon. The Principal Legal Advisor, Office of General Counsel, FBIHQ, or the United States Attorney's Office should be consulted if questions arise regarding whether an Agent's weapon should be surrendered to local authorities.

(5) The SAC or ASAC will initiate a personal contact with the Agent(s) and his/her family in a supportive role and offer assistance, if needed. This contact will be made as soon as possible following the incident (within the first 24 hours).

(6) The current Bureau procedure of not releasing the identity of Agents involved in investigations or incidents is especially important in post-shooting matters and will be maintained.

(7) An SAC should communicate with FBIHQ if any of the established procedures appear to be inappropriate for a specific incident.

(8) SACs and/or ASACs should hold an office conference, as soon as practical, after a shooting incident and as often as necessary to keep all personnel advised of pertinent details concerning the shooting incident. This should substantially reduce rumors and distorted accounts of the incident. (See MAOP, Part II, 8-1.3.2.)

EFFECTIVE: 05/20/94

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 36

12-11.3 Guidelines For Intervention During The First Week (See  
MAOP, Part II, 8-1.3.2.)

(1) The Critical Incident Program consists of several specifically trained Agents and support employees located at the FBI Academy, Quantico, Virginia, and throughout the field offices administered from Personnel Division (PD), FBIHQ.

(2) The Critical Incident Program also includes FBI Chaplains in each field office who have been trained to respond to Agents and support employees who have been involved in critical incidents including shootings.

(3) Bureau policy establishes confidentiality for any conversations between employees and peer support employees or FBI Chaplains.

(4) There are exceptions to this Bureau policy of confidentiality which could require disclosure. These exceptions might include, but are not limited to, risk of death or injury, perspective criminal acts, or interference with Bureau investigations. A decision to disclose must first be discussed with the Critical Incident Program Manager, PD, FBIHQ. No assurance can be given that the courts will recognize the confidential relationships established by this policy. In a criminal or civil action arising from a critical incident, the court could conceivably order disclosure notwithstanding Bureau policy.

(5) The SAC or ASAC will advise the office FBI Chaplain(s) of the critical incident and coordinate a request for peer support with the PD, FBIHQ.

(6) A brochure is available to Agents/employees who have been involved in shooting incidents covering:

- (a) The symptoms to be expected and their normal course.
- (b) Administrative handling of the post-shooting investigation.
- (c) Legal aspects of the shooting incident.
- (d) Counseling services available.

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 37

(7) An official from FBIHQ will contact the Agent personally by telephone. The scope and direction of this call is to express concern for the welfare of the Agent and his/her family. The Assistant Director, PD, will coordinate the personal phone contacts.

(8) A total of five optional days of administrative leave are available to be taken (at sole discretion of) persons directly involved in the shooting incident. The use of that administrative leave will be strongly encouraged by the SAC. This leave may be taken at any time at the discretion of the Agent and should be coordinated with his/her supervisor. The Health Care Programs Unit (HCPU), PD, will furnish guidance concerning individuals eligible for leave and authority to grant leave. (Also see LEAVE ADMINISTRATION GUIDE.)

(9) An Agent directly involved in the shooting incident should be advised by the SAC that the Agent can be reassigned from his/her squad for a period of time if the Agent so desires.

(10) The SAC will immediately coordinate with HCPU, PD, FBIHQ, if an Agent directly involved in the shooting incident requires other special attention, to initiate the utilization of the mental health professional resources of the Employee Assistance Program (EAP).

(11) If an Inspector has been assigned to conduct the shooting inquiry, he/she will review these intervention guidelines with appropriate field office managers.

(12) In the event of an incident which involves the death of an employee or a line-of-duty injury that results in the hospitalization of the employee for serious injuries, the Director desires to personally contact the employee or family and offer comments that will contribute, even if in only a small fashion, to the healing process that lies ahead. To facilitate these contacts the following information should be relayed to the Director expeditiously, usually by teletype.

(a) A brief description of the incident and the nature of the injuries sustained.

(b) The name(s) and age(s) of the employee's immediate family.

(c) Where and when the employee or family may be reached.

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 38

(d) Any other information that would be helpful during the Director's contact with employee or family.

(13) Recognizing that the FBI's continuing concern can significantly help the recovery of our employees and their families, it may be beneficial for the Director to recontact them. The timing of this recontact is left to the discretion of the SAC. Recontact requests should be submitted by teletype to the Director's personal attention and include the following information:

(a) The information requested above.

(b) An update on the condition of the employee or family.

(14) More periodic expressions of concern by the immediate FBI family will be led by the SAC. SACs should be aware of the extensive support structure that exists in the HCPU of the PD. This includes peer support, contract mental health professionals, FBI Chaplains and the EAP. These resources should be used as appropriate to provide our employees and their families with the support and assistance they need during times of extreme trauma and sorrow.

EFFECTIVE: 05/20/94

12-11.4 Guidelines for Long-Term Issues (See MAOP, Part II, 8-1.3.2.)

(1) SAC or ASAC will personally make every effort to facilitate the administrative investigation of a shooting incident.

(2) If a group of Inspectors from FBIHQ is required to conduct an investigation of the shooting incident, an effort will be made to ensure that at least one of the Inspectors has received training in the effects of post-shooting trauma and, if possible, has personally experienced a shooting incident.

(3) Agents should be allowed to pace their own return to work following shooting incidents. The Personnel Division (PD) will furnish guidelines concerning use of administrative leave. The SAC and supervisor will be involved in this decision-making process.



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 39

(4) If a transfer of an Agent to another squad following a shooting incident is contemplated, consideration will be given to the effects of the transfer on the adjustment period and the Agent should be involved in the decision.

(5) The letter announcing the conclusion of a Bureau investigation of a shooting incident will be phrased in a way that takes into account the emotional impact on the Agent who has been involved in a life-threatening situation and may have suffered post-shooting trauma.

(6) SACs and/or ASACs or the Principal Firearms Instructor should personally and individually provide the necessary positive and/or negative feedback to Agents after the administrative inquiry has been completed. This will also afford an opportunity to ascertain if the involved Agent(s) is amenable to any formal recognition, as warranted. Medals or incentive awards following a shooting incident in which subjects have been seriously injured or killed can have a negative psychological impact and/or be perceived as a reward. However, medals or incentive awards may be appropriate, and will be authorized if recommended and justified. Emphasis will be on the effort to save lives.

(7) Agents who have been involved in a shooting incident will not immediately be assigned to duties likely to involve armed confrontations. This is even more important when a given Agent has already been involved in a previous shooting incident. This consideration should take precedence over other action, including transfers.

(8) Employees who have been involved in shooting incidents will be afforded an opportunity to attend a Post-Critical Incident Seminar at the FBI Academy. These group sessions will be the basis for future modifications in policy and training and will also provide a pool of employees able to provide meaningful peer support. The group sessions provide a therapeutic understanding of the shooting event. These conferences will be coordinated by the Training Division's Behavioral Science Services Unit (BSSU).

(9) PD's Employee Benefits Unit has prepared a booklet captioned "Your Worker Compensation Benefits" for questions relating to work-related illnesses and injuries.

(10) The PD Transfer Ombudsman had been designated to serve as a single point of contact at FBIHQ concerning insurance and compensation matters following a shooting incident. The Ombudsman

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 40

will be available on a case-by-case basis to respond following a critical incident and offer assistance to victims and survivors of that incident concerning insurance and compensation matters. The Ombudsman attends Post-Critical Incident Seminars and maintains contact with the Critical Incident Program Manager.

(11) Six months after the shooting incident, HCPU, PD, FBIHQ, will contact the SAC of the Agent involved in the shooting incident to determine if follow-up counseling is necessary.

---

EFFECTIVE: 05/20/94

12-11.5 Guidelines For Training (See MAOP, Part II, 8-1.3.2.)

(1) Training related to post-shooting trauma and its management will be made available to Bureau administrative personnel. A training block of this type will be presented by the Behavioral Science Services Unit, (BSSU), Firearms Training Unit, and the Management Science Unit, Training Division. A presentation in this area should also be incorporated into upcoming SAC Conferences, Senior Executive Programs, and Executive Development Institute sessions.

(2) An orientation session by the BSSU on an introduction to post-shooting trauma will be provided to students during New Agents training.

(3) In the planning of operations which have a high risk of armed confrontations and/or may involve the use of deadly force, if the SAC, ASAC or supervisor is aware of an Agent who is experiencing high levels of personal and/or family stress or health problems, consideration should be given to temporarily excuse the SA from participating in the exercise in order to minimize the risk of cumulative stress or trauma incidental thereto.

EFFECTIVE: 05/20/94

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 41

12-11.6 Nondisclosure of Agents' Names in Shooting Incidents (See MAOP, Part II, 5-2 (4) and 8-1.3.2.)

Names of Agents involved in shooting incidents in performance of duty should not be volunteered to outsiders since experience has shown that once their identities become a matter of public knowledge, the potential that they and their families will be subjected to harassment and possible retaliation substantially increases. If identities of Agents involved in shooting incidents have been made public through inclusion in public records or disclosure at public proceedings, SACs may verify the Agents' identities in response to inquiries by news media representatives or others.

EFFECTIVE: 04/07/97

12-11.7 Investigation of Shootings Involving FBI Personnel (Formerly 12-11.1.) (See MAOP, Part II, 8-1.3.2.)

(1) An investigative inquiry of the shooting incident will be conducted under the direction of the SAC or Inspector/Inspector in Place (IIP), as appropriate, and a comprehensive report issued.

(a) The SAC is responsible for preserving evidence and instituting a logical investigation. SAC or SAC's designee should personally coordinate investigation if an Inspector/IIP is not dispatched to the scene.

(b) The SAC will designate an investigative team to conduct those shooting inquiries under his/her direction. The SAC should use appropriate personnel and resources (Evidence Response Team (ERT), Photographer, etc.) to conduct a thorough, factual investigation of the shooting incident and to submit a comprehensive report to the Shooting Incident Review Group (SIRG). The SAC should consider Laboratory Division assistance in appropriate circumstances.

(c) In the event an Inspector/IIP is dispatched to the scene, the Shooting Incident Response Team (SIRT) will be comprised of an Inspector or IIP and two or more Assistant Inspectors-in-Place (AIIP) selected by the Chief Inspector, Inspection Division

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 42

(INSD), and a forensic team comprised of a firearms examiner, visual information specialist, and photographer selected by the Laboratory Division.

(d) The SIRT under the direction of the Inspector or IIP will report directly to the Chief Inspector, Office of Inspections, during the shooting inquiry and be tasked with completion of a thorough, factual investigation of the shooting incident and submission of a comprehensive report to the SIRG, along with any observations regarding safety and/or training issues identified through the inquiry.

(2) Local authorities are to be contacted to clarify jurisdiction and investigative responsibilities.

(3) All personnel and witnesses at the scene are to be identified, located and interviewed.

(4) Agents involved in a shooting must be given sufficient time to regain composure before being requested to provide any statements. The official conducting the inquiry will consult with the SAC or other appropriate personnel and consider such factors as physical injuries or trauma experienced by the Agent involved in a shooting to determine when an interview should take place.

(5) Avoid having involved Agent(s) conduct any investigation and/or interviews relevant to the shooting. Do not, however, delay substantive investigation to accomplish this. Separate and remove involved Agent(s) from the scene as soon as practical.

(6) Forms FD-644 (Warning and Assurance to Employee Requested to Provide Information on a Voluntary Basis) and FD-645 (Warning and Assurance to Employee Required to Provide Information) are not to be used in investigations concerning shooting incidents in the absence of specific, compelling reasons. Such a determination will be made by the SAC or Inspector/IIP in consultation with the appropriate FBIHQ officials. Prior to the use of the FD-645 in cases where there is potential for criminal prosecution of the employee to be interviewed, OPR, Inspection Division, must present the facts of the case to OPR, DOJ, and obtain an initial opinion that the matter in question should be handled administratively rather than criminally. (See MAOP, Part I, 13-6 (3) and MIOG, Part I, 263-5 (3).)

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 43

EFFECTIVE: 10/17/95

12-11.8 Shooting Inquiry Report (See MIOG, Part II, 12-11.1;  
MAOP, Part II, 8-1.3.2.)

(1) Results of an inquiry in all shooting incidents involving the intentional use of force by FBI personnel and in all incidents, intentional or otherwise, WHERE INJURY OCCURS, are to be submitted to FBIHQ within two weeks in the form of an investigative report. The shooting inquiry is primarily a fact-finding effort and must be objective, thorough, and factual. Observations regarding safety and/or training issues identified during the inquiry should be included in the report.

(2) Report should be captioned "Shooting Inquiry, Report of Shooting Incident; (name of Reporting) Division; (date of shooting incident); Admin Matters; (66F classification)." The report should specifically reference, using case caption, the substantive violation, if any, involving the shooting incident, e.g., "John Doe; First Savings Bank; 3/6/95; BR; OO: NY; UCFN #." Reference should also be made to the teletype that initially advised FBIHQ of the shooting and the communication which forwarded the FD-418s.

(3) The report should contain appropriate enclosures and exhibits, to include but not limited to: medical reports, coroner or autopsy reports, police reports, crime scene diagrams, radio logs, criminal record and NCIC checks, military records of subjects if pertinent, weather information, firearms and ballistic information (include Laboratory Reports if available or FD-302 summary of laboratory analysis), videos from local news media, shooting incident reconstructions, and crime scene photographs.

(4) No accomplishments should be claimed in the Shooting Inquiry report. Any accomplishments achieved at the time of the shooting incident should be claimed by a communication under the substantive title.

(5) The Administrative section of the report should include information concerning decisions regarding interview of subject(s), pertinent administratively controlled material, informant information, and observations regarding training and/or safety issues. SAC analysis and recommendation(s) for administrative action, if deemed warranted, should be set forth in this section of the report.

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 44

(6) A table of contents should be utilized to organize and identify report contents. Following is an example of items which might normally be included:

(a) Interviews of personnel involved - include signed, sworn statements of all Bureau employees principally involved in the shooting incident. Interview all Bureau personnel directly involved in the investigation and/or planning leading to the shooting incident. Any arrest or raid plans pertinent to the incident should be carefully spelled out in statements obtained from the person(s) in charge of the raid/arrest.

Interviews in shooting inquiries should be handled without the use of Forms FD-644 and FD-645, unless there are specific factual situations or complaints which might raise concerns about the shooting. Should these arise, the details should be discussed with the Chief Inspector, Inspection Division (INSD), prior to conducting any interview of Bureau personnel.

(b) Interviews of witnesses - include FD-302s of all witnesses to the shooting incident. Persons interviewed should be apprised of the access provisions of the Privacy Act and afforded the opportunity to request confidentiality in accordance with MIOG, Part I, 190-7 and SAC Memo 51-77 (C) dated 11/15/77.

(c) Investigation regarding subject(s) - include such information as criminal records, if available, and interviews of associates which are germane to shooting (i.e., individuals involved in circumstances surrounding the shooting incident, co-arrestee, etc.). If possible, include interview of subject(s) regarding the shooting. Such an interview is often quite productive in obtaining admissions from the subject(s) directly pertinent to the shooting incident. Statements made by subject(s) contemporaneous to the shooting oftentimes may be important to the overall evaluation of the incident by the SIRG.

Apprehension FD-302 should be included. Prepare FD-302 reporting that subject did not, was not known to have, or refused to comment on the shooting, if applicable.

(d) Medical reports - include medical reports and interviews with medical personnel clarifying the nature and gravity of all wounds or injuries as a result of the shooting. Indicate weapon, entry and exit of individual shots, if determinable. If fatalities involved, include coroner or autopsy reports.

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 45

(e) Vehicles involved - describe all pertinent vehicles and indicate damage incurred. Describe any other property damage.

(f) Weapons involved - include FD-302s reflecting weapons and ammunition used by Agent(s), officer(s) and subject(s) involved and disposition or custody of weapons following the shooting.

(g) Maps, diagrams, photographs, and other graphic depictions or representations of shooting incident scene and/or scenario.

(h) Police reports - include copies of reports, if available, plus any statements made regarding possible prosecutive action against Bureau personnel. Include copy of communications with local prosecuting attorney.

(i) Prosecutive status of subjects.

(j) Laboratory reports - laboratory reports should be included in the Shooting Inquiry report, if they are available. If laboratory examinations have not been completed, preliminary results should be reported by a summary FD-302. Results of forensic processing conducted at the scene may be included in the form of a laboratory report or an FD-302, whichever is deemed most suitable by the forensic expert(s).

(7) To assure accuracy and completeness of the Shooting Inquiry report, SAC or Inspector/IIP should confer with the Chief Inspector, Office of Inspections, INSD.

(8) Submit an original and 12 copies of the report to the Assistant Director, INSD, Rm. 7129, Attention: SIRG, with one copy designated to the FTU. The INSD will distribute copies to members of the SIRG.

EFFECTIVE: 10/17/95

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 46

12-11.9 Shooting Incident Review Group (Formerly 12-11.1.) (See  
MAOP, Part II, 8-1.3.2.)

(1) The Shooting Incident Review Group (SIRG) is an independent review committee established to analyze all shooting incidents involving Bureau personnel and to evaluate the application of deadly force in such incidents. The SIRG is to provide the Director with an evaluative analysis, observations, and recommendations for corrective actions from an operational standpoint, if any, as well as recommendations concerning training issues, safety issues and administrative action, if deemed necessary.

(2) Scope and Purpose: The SIRG will review all shooting incidents wherein Bureau personnel employ deadly force, as well as all incidents where a firearm is discharged in a nontraining setting.

(a) The SIRG will determine if the shooting under review was intentional or unintentional. This will govern the standards applied in the review as the FBI's Deadly Force Policy will only be applied where the shooting was intentional.

(b) The SIRG will deliberate and determine if the shooting incident falls within the application of the FBI's Deadly Force Policy and the law.

(c) The SIRG will review operational plans, procedures, tactics and circumstances leading to the shooting incident.

(d) The SIRG will review issues associated with safety, training, and management oversight and make recommendations for administrative action, if deemed necessary.

(3) The SIRG will be comprised of representatives from the following:

(a) Inspection Division (INSD) - Deputy Assistant Director, (Chairperson) and Chief Inspector, Office of Inspections, (Alternate Chairperson);

(b) Criminal Investigative Division;

(c) National Security Division;

(d) Training Division;



Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 47

(e) Personnel Division;

(f) Office of the General Counsel;

(g) Laboratory Division;

(h) Field Supervisor (preferably one who has been involved in a shooting incident) from the Washington, D.C. Metropolitan area.

(i) Department of Justice Attorney(s) as delegated by the Deputy Attorney General.

(4) The SIRG will deliberate and report its analysis by issuing a memorandum of findings and recommendations to the Director. This memorandum will be reviewed by the SIRG members, each of whom may provide additional comments, observations, or recommendations by attaching an addendum to the memorandum.

(5) The findings and recommendations will be submitted from the SIRG by the Chairperson to the Assistant Director, INSD, for approval and forwarding to the Director. An information copy of the SIRG memorandum of findings will be disseminated to the substantive Assistant Director (CID or NSD) as appropriate, and to other appropriate entities (Training, Personnel, etc.).

EFFECTIVE: 10/17/95

12-12 HOLSTER/ACCESSORY EQUIPMENT

(1) SAs must train with holsters and related equipment normally used on duty at each firearms training session.

(2) Holsters are not provided for personally owned weapons.

(3) Personally owned holsters must be approved through the PFI before use.

(4) Alterations of any holster, such as removing a thumb brake, is not permitted.

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 48

(5) Accessory equipment, i.e., magazine or speed loader pouches, ammunition pouches, etc., must be maintained and inspected in the same manner as a holster.

(6) Each SA is responsible for the proper maintenance of all holsters and accessory equipment under his/her control.

(7) Bureau-issued holsters/accessories, when worn or damaged beyond repair may be replaced through the FBI Academy Gun Vault.

(8) All strong side belt holsters will meet the following requirements:

(a) Must be able to draw and reholster the handgun with one hand.

(b) The holster must not require the trigger finger to pass through the trigger guard to release the weapon.

(c) the holster must secure the weapon during strenuous physical activity (running, climbing, upside down, etc.).

(9) "Miscellaneous holsters" refers to shoulder holsters, belly bands, ankle holsters, inside pants holsters, cross-draw holsters, fanny (butt) packs, etc.

(a) All regulations that exist for strong side hip holsters apply with the exception that it is permissible for the weak hand to steady the holster while returning the weapon. However, no holster will be approved that REQUIRES using both hands to draw the weapon.

(b) Firearms instructors are to ensure that proper safety is exercised during training with any miscellaneous holster.

(10) SAs should use both Bureau-issued and personally owned holsters and other firearms equipment during firearms training sessions to ensure familiarity.

EFFECTIVE: 04/07/97

XXXXXX  
XXXXXX  
XXXXXX

FEDERAL BUREAU OF INVESTIGATION  
FOIPA  
DELETED PAGE INFORMATION SHEET

9

Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

- Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552

Section 552a

(b)(1)

(b)(7)(A)

(d)(5)

(b)(2)

(b)(7)(B)

(j)(2)

(b)(3)

(b)(7)(C)

(k)(1)

(b)(7)(D)

(k)(2)

(b)(7)(E)

(k)(3)

(b)(7)(F)

(k)(4)

(b)(4)

(b)(8)

(k)(5)

(b)(5)

(b)(9)

(k)(6)

(b)(6)

(k)(7)

- Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

- Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

Pages were not considered for release as they are duplicative of \_\_\_\_\_

Page(s) withheld for the following reason(s): \_\_\_\_\_

- The following number is to be used for reference regarding these pages:

MIOG Pt II Sec 12 p49 thru 57

XXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X for this page X  
XXXXXXXXXXXXXXXXXXXXX

XXXXXX  
XXXXXX  
XXXXXX

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 58

12-15 DEMONSTRATIONS AND TOURS

(1) Only authorized firearms instructors may present "live fire" demonstrations, and then only with the express consent of the SAC or designee.

(2) Any other SA may present Bureau firearms for demonstration using "red-handle" weaponry or live weapons equipped with trigger guard locks or similar devices which prevent the weapon from firing.

(3) The safe condition of all weapons used for demonstration should be verified by a Bureau firearms instructor BEFORE use. (The general safe condition of firearms is action open, safety on, and weapon free of any live ammunition.) Demonstration weapons should never be pointed at another person.

EFFECTIVE: 04/07/97

12-16 MEDICAL PROFILE SYSTEM - MEDICAL MANDATES (RESTRICTIONS)

(1) Agents on medical mandates are to be permitted to participate in firearms training, including defensive tactics, PROVIDED the Agent's evaluating physician is fully familiar with the Agent's condition, the nature of the training to be undertaken, and furnishes a written statement that, in the physician's opinion, such participation would not be injurious to the Agent's health or dangerous to others. (See MAOP, Part I, 20-5.2.1 (2).)

(2) In instances where the evaluating physician does not certify the Agent to attend training and the prospects for future participation are remote due to the Agent's condition, authority to carry a firearm will be rescinded and any Bureau-issued weapon turned in. (See MAOP, Part I, 20-5.2.1 (3).)

EFFECTIVE: 04/07/97

Sensitive  
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 59

12-17 TRAINING SAFETY

(1) All training exercises or scenarios which incorporate the use of loaded or unloaded firearms must be supervised by a currently qualified Bureau firearms instructor.

(2) The supervising firearms instructor must ensure that:

(a) all necessary firearms and ammunition safety checks are conducted prior to commencement of training.

(b) all firearms safety rules and precautions are adhered to by all participants.

(c) all facilities and training props are safe and absent of potential hazards to all personnel.

(3) The primary instructor may designate assistants as required; however, the ultimate responsibility for safety rests with the primary instructor.

(4) Under no circumstances will the primary or assistant instructors become active participants or role players during the training exercise or scenarios.

EFFECTIVE: 04/07/97

12-17.1 Deleted

EFFECTIVE: 04/07/97

12-17.1.1 Deleted

Sensitive

Manual of Investigative Operations and Guidelines  
Part II

PAGE 12 - 60

EFFECTIVE: 04/07/97

| 12-17.1.2 | Deleted |

EFFECTIVE: 04/07/97

| 12-17.1.3 | Deleted |

EFFECTIVE: 04/07/97

Sensitive  
PRINTED: 02/18/98