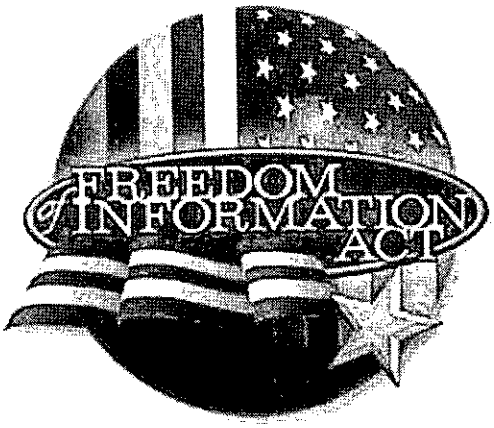
FOIPA COVER SHEET

FREEDOM OF INFORMATION AND PRIVACY ACTS

SUBJECT: MANUAL OF INVESTIGATIVE OPERATIONS AND GUIDELINES (MIOG)

UPDATES

PART 2 VOL.1



FEDERAL BUREAU OF INVESTIGATION

THE BEST COPY OBTAINABLE IS INCLUDED IN THE REPRODUCTION OF THESE DOCUMENTS. PAGES INCLUDED THAT ARE BLURRED, LIGHT, OR OTHERWISE DIFFICULT TO READ ARE THE RESULT OF THE CONDITION OF THE ORIGINAL DOCUMENT. NO BETTER COPY CAN BE REPRODUCED.

MANUAL OF INVESTIGATIVE OPERATIONS AND GUIDELINES

PART II

VOLUME I

TABLE OF CONTENTS

SECTION	
7	INTERVIEWS
10	RECORDS AVAILABLE AND INVESTIGATIVE TECHNIQUES
11-5	EMERGENCY AND PURSUIT DRIVING
12	FIREARMS

SECTION 7. INTERVIEWS

7-1 USE OF CREDENTIALS FOR IDENTIFICATION

Credentials (commission cards) shall be exhibited to all persons interviewed by Special Agents so there will be no doubt concerning the organization with which they are connected.

EFFECTIVE: 01/08/79

7-2 THOROUGHNESS, PRECAUTIONS, TELEPHONIC AND USE OF INTERPRETERS

EFFECTIVE: 01/08/79

7-2.1 Thoroughness and Precautions During Interviews

(1) When interviewing subjects and suspects, consideration should be given to including questions as to the knowledge on the part of the interviewee of previous crimes of a type similar to the one currently being investigated. The objective is to develop information concerning other unsolved violations.

(2) In the interrogation of subjects and suspects of Bureau investigations, all Agents should be most meticulous not to disclose directly or indirectly confidential informants or confidential sources of information. Questions or references to papers and files may enable an intelligent subject to fix the source of our information.

(3) During an interview with a witness, suspect, or subject, Agents should under no circumstances state or imply that public sentiment or hostility exists toward such person. If, during an interview with a witness, suspect, or subject, questions are raised by such persons, or if anything transpires which gives reasonable grounds to believe that subsequently such questions or incident may be used by someone in an effort to place an Agent or the Bureau in an unfavorable light, a memorandum regarding such questions or incident should be immediately prepared for the SAC. The SAC is responsible

for promptly advising FBIHQ and the USA of such questions or incident and FBIHQ must be promptly informed of all developments.

(4) Agents are not acting as practicing attorneys and under no circumstances should legal advice be given or an attempt made to answer legal questions. Agents who are attorneys should not deliberately make known their legal training. If an Agent who is an attorney is questioned regarding|his/her|legal training,|Agent|should state that|he/she|is an attorney but that|he/she|is not in a position to give legal advice or answer legal questions. Agents should not interview subjects, subsequent to the initial interview, to determine what plea subject will make on arraignment. If a USA should make such a request,|USA|should be informed of FBIHQ instructions.

EFFECTIVE: 01/08/79

7-2.2 Telephone Interviews

Interviews and investigations by telephone are highly undesirable. However, in those few instances in which a substantial saving of time would be effected and the necessary information can be fully obtained, the use of the telephone may be justified. The SAC must personally approve the use of the telephone to conduct interviews and investigations in every instance.

EFFECTIVE: 01/08/79

7-2.3 Use of Interpreters

When subjects cannot converse in English adequately, make arrangements to have interpreter present. Use Bureau personnel if available in same or adjacent office. Otherwise, qualified interpreters from other U.S. intelligence or enforcement agencies may be used. If none of foregoing available, consider use of sponsor or close relative of subject for exploratory interview, leaving way open for reinterview with qualified interpreter if all questions cannot be resolved. If qualified interpreter is necessary and is not available, request FBIHQ assistance.

EFFECTIVE: 01/08/79

7-3 REQUIRING FBIHQ AUTHORITY

FBIHQ authority to interview is required before interviews are conducted in the following instances:

(1) The individual to be interviewed is prominent and/or controversial and suspected of a crime and/or the investigation may receive extensive media coverage.

(2) The individual is an employee of the news media who is suspected of a crime arising out of the coverage of a news story or while engaged in the performance of his/her duties as an employee of the news media. Attorney General authority is also needed. (See MAOP, Part II, 5-7, for further information.)

(3) Refer to FCIM, Part I, 0-2.5 for FCI investigations.

(4) In other matters, the need for FBIHQ authority is set forth in the guidelines dealing with a particular type of case.

(5) Whenever a question arises as to whether or not FBIHQ authority must be obtained prior to an interview, it should be resolved in favor of contacting FBIHQ.

EFFECTIVE: 01/08/79

7-4 ONE VS TWO AGENT INTERVIEW OF SECURITY SUBJECT

Safety, security, sensitivity and good judgment are considerations in evaluating necessity for two Agents to conduct interview of any subject in all types of security investigations. SACs have responsibility and option of deciding when two Agents should be present during any interview of this nature. Safety of Specials Agents should be first priority in any evaluation in this regard.

EFFECTIVE: 01/08/79

7-5 EVALUATION OF AN INTERVIEW

An interview cannot be considered thorough unless the account thereof shows the basis for allegations or other pertinent information furnished by the source during the interview. Only with the benefit of these important details can the information be fully and properly evaluated. Statements or allegations may not be accepted without inquiring of the source as to how source acquired such information, or as to the basis for beliefs or opinions he/she might express. If his/her information is based on hearsay, an effort must be made to identify the original source and to interview that source if feasible to do so. In this regard, consideration must be given to protection of the identity of confidential Bureau informants or sources when necessary. When details as to the basis for allegations made or the identity of original sources if disseminated outside the FBI would tend to reveal the identity of an individual whose identity should be protected, that fact should be called to attention and those details furnished by cover page(s). For example, A furnishes the New York Office pertinent information, orally or in writing, which A said he/she received from B. The body of New York's report must clearly show that A cannot personally attest to the accuracy of the information, but that he/she received it from another individual; however, B should not be named in the body of a report unless the New York Office knows there is no objection to the disclosure of B's name. Whether B is identified by name or not, the body of the report must contain any available description of B to permit an evaluation of the information being reported. These requirements are applicable to interviews of all types, including established FBI sources or informants, subjects, suspects, and witnesses, and to all types of Bureau investigations. Written statements by informants are not to be considered an exception. The basis for statements attributed to established sources and confidential informants need not be set out in investigative reports provided informants' statements or channelizing memoranda specifically show the information is based on personal knowledge of the informant. If it is not of informant's personal knowledge, the investigative report must show the basis for informant's statements. Any deviation from these requirements should be called to FBIHQ's attention and fully justified. Failure to comply without sufficient justification will be considered a substantive error for which administrative action will be considered.

EFFECTIVE: 10/23/86

7-6 INTERVIEWING COMPLAINANTS AND SUBJECTS OF CRIMINAL INVESTIGATIONS

EFFECTIVE: 10/23/86

7-6.1 Interviews of Complainants

(1) Complainants who have transmitted information to FBIHQ by letter and who have been advised that they would be interviewed in the field must be interviewed promptly and appropriate advice submitted to FBIHQ. Delay in handling the interview must be reported to FBIHQ.

(2) Complainants who have communicated with field offices must be interviewed promptly when they have been advised that an Agent would interview them.

EFFECTIVE: 10/23/86

7-6.2 Subjects of Criminal Investigations

|(1)| In interviews with subjects and suspects, consideration is to be given to the solution of crimes other than the one which is presently being investigated.

|(2)| In such interviews, the disclosure of the identity of confidential informants and confidential sources of information must be avoided.

|(3)| In interviewing subjects of criminal investigations where the possibility exists the subject may have evaded payment of income taxes or there is an apparent irregularity relating to the payment of income taxes, consideration should be given to inquiring of the subject as to whether|he/she|filed an income tax return for the pertinent period and where it was filed. Such an inquiry should not be made where there is a possibility that it will prejudice our case. If any information of interest to the Internal Revenue Service, Treasury Department, is obtained as a result of such an inquiry, it should be promptly referred to the local office of the Internal Revenue Service, and to FBIHQ in a form suitable for dissemination.

EFFECTIVE: 10/23/86

7-7 DEVELOPMENT OF DEROGATORY INFORMATION DURING INTERVIEWS

Derogatory data developed through interviews of witnesses and other sources must be completely approved or disproved and accurately and factually established as applicable to the person under investigation. The danger of relying upon information obtained from one source is obvious and vigorous steps must be taken to further develop such cases through evidence obtained through other sources and from various investigative techniques. Beware of being misled by circumstantial evidence and guard against incomplete interviews or overeager witnesses who deviate from telling what they actually know to what they erroneously feel the FBI is desirous of obtaining.

EFFECTIVE: 02/20/90

7-8 IDENTIFICATION OF SUSPECTS

Identification of suspects by witnesses interviewed should be in crystal-clear, unmistakable language, showing exact basis for such identification, and corroboration should be developed for same wherever possible. Make certain that when suspects are identified in a lineup the identification is from independent knowledge and recollection of the facts by the witnesses, and not from the witnesses' mere association with the suspect with a photograph of the suspect previously exhibited to the witnesses. There is no "margin of error" allowed the FBI for mistaken identifications. Obtain a signed statement whenever it is possible in those instances in which a witness, who would or could subsequently testify, makes a positive identification of a subject from a photograph or by personal observation. |Investigators may wish to utilize Form FD-747, Photo Spread Folder, to display the photographs.| If witness refuses to|provide a signed|statement, so indicate in the report.

EFFECTIVE: 02/20/90

7-9 INTERVIEWS INVOLVING OR RELATING TO COMPLAINTS

EFFECTIVE: 02/20/90

7-9.1 Complaints Received at the Field Office

Complaints must be handled by the SAC, ASAC, or supervisory staff in all offices which do not have an authorized complaint desk. If the information in the complaint will result in publicity or if FBIHQ may be interested, FBIHQ should be advised promptly.

EFFECTIVE: 02/20/90

7-9.2 Complaints In Person or By Telephone

(1) The employee receiving the complaint must complete Form FD-71 immediately. However, the preparation of the complaint form is not necessary in those instances in which immediately upon receipt of the complaint a teletype, airtel or letter is sent out the same day to another field office or FBIHQ setting forth the essential facts of the complaint. Any details which normally would appear on the complaint form which are not contained in the body of such teletype, airtel, or letter are to be added to the yellow file copy so that complete data will be available in the files of the office where the complaint was received. FD-71 is a letter-size preinserted carbon white form made up so that the name and aliases of the subject, address, character, name of the complainant, address, phone number, personal or telephonic, date and time, subject's description, facts, and name of employee receiving the complaint can be entered and the results of the indices check can be shown.

(2) The index must be checked immediately regarding names of complainant (unless complainant is a known or established source) and subject. The SAC must indicate action to be taken. Proper consideration must be given to all persons who contact field offices either telephonically or personally whether as complainants or visitors. Such contacts must be handled courteously and promptly and there must not be any improper, indifferent, or arrogant treatment of such contacts.

EFFECTIVE: 02/20/90

7-9.3 Complaints By Letter

(1) Concerning a matter not within the jurisdiction of the FBI but within the jurisdiction of some other Federal investigating agency, acknowledge the letter of the complainant to the proper agency. (Form FD-342 may be used to transmit anonymous letters.) If complaint concerns a matter handled by Department of Labor under Labor-Management Reporting and Disclosure Act 1959, advise complainant in acknowledgement that the matter has been referred to the USA for appropriate action. Immediately upon referral to USA include information in an LHM and forward to FBIHQ.

(2) Incoming communications must be acknowledged promptly, except where SAC deems otherwise.

EFFECTIVE: 01/31/78

7-9.4 Complaints Critical of the FBI or Its Employees

(1) Complaints received critical of employees or the FBI must be thoroughly investigated and promptly reported to FBIHQ.

(2) Upon receipt of a critical complaint about the FBI from a public official which necessitates an inquiry to ascertain the facts prior to acknowledging the communication, the SAC, or in his absence whoever is acting for him, must promptly call the public official, acknowledge receipt of the communication, state that a prompt inquiry is being initiated to ascertain the facts, and that as soon as all the facts are secured the SAC will be in touch with the complainant. If there is any question in the mind of the SAC, or whoever is acting for him, as to the propriety of this, immediately communicate with the appropriate official of FBIHQ so that the matter can be resolved.

EFFECTIVE: 01/31/78

7-9.5 Legal Requirements of the Privacy Act of 1974 (Title 5, USC, Section 552a)

When conducting an interview for any purpose, the interviewing Agent must always bear in mind the provisions of the Privacy Act, i.e., information collected must be: (1) relevant and necessary to accomplish a purpose of the Bureau; (2) authorized to be accomplished by statute or Executive Order of the President (or by the Constitution).

Additionally, the information collected must be accurate, relevant, timely, and complete; and, if describing how an individual exercises a right guaranteed by the First Amendment to the Constitution, the collection and maintenance of the information must be pertinent to and within the scope of an authorized law enforcement activity.

For a more detailed explanation of these provisions, refer to Section 190-5 of this Manual.

EFFECTIVE: 01/31/78

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

10-2 RECORDS AVAILABLE

[redacted]

Biographic Directories
[redacted]

City Directory
Closed and Pending Files
Court System
[redacted]

Department of Veterans Affairs
[redacted]

Field Office Special Services List
[redacted]

Government Agencies
[redacted]

Identification Records (FD-9)
[redacted]

Interstate Identification Index
[redacted]

Maps
Marriage Records
Merchant Marine
Military Departments
Motor Vehicle Department
[redacted]

National Auto Theft Bureau
Newspaper Library
[redacted]

PD Checks
[redacted]

Probation and Parole Offices
Public Libraries
[redacted]

b2
7E

Schools and Colleges
Social Security Records
Sources of Information Index
Street Guide
Surveillances
[redacted]
Telephone Directory
[redacted]
Unemployment Agencies, Federal and State
[redacted]
Voter Records

b2
7E

EFFECTIVE: 05/25/90

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

Authorship Identification	Authorship identification is an examination of aural (recordings), written or printed material to determine a subject's age, ethnic, geographical or educational idiosyncrasies. (See MIOG, Part II, 13-28.)
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
- 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

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, 13-18

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 - 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: 09/03/93

10-4 COMPUTER ASSISTANCE OR AUTOMATIC DATA PROCESSING

The Systems Development Section (SDS) of the Technical Services 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: 11/17/88

-5 INTERSTATE IDENTIFICATION INDEX (III)

(1) The III allows on-line accessibility of more than twelve million 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.

(2) Detailed instructions for conducting name searches 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 Identification Division since it maintains over 13 million additional manual records.

EFFECTIVE: 11/17/88

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

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.

EFFECTIVE: 03/09/81

10-6.2 Policy

(1) FBIHQ approval must be obtained before a mail cover request is submitted to the USPS.

(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 FBIHQ approval of 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. FBIHQ is to be notified upon the termination of each mail cover. FBIHQ is also to be notified if request for mail cover is not approved by the Postal Service, which notification shall include a statement of the reasons given by the postal authorities for not approving the 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 Security/Terrorism Investigations," effective 3/21/83.)

(8) A mail cover index is to be maintained by the Support Services Supervisor|(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: 01/21/86

10-6.3 Requesting FBIHQ Approval

EFFECTIVE: 05/10/82

10-6.3.1 Fugitive or Criminal Cases

(1) In recommending a mail cover in a fugitive or criminal case, submit an airtel to FBIHQ advising that UACB within ten days your office intends to request a mail cover from the district Postal Inspector in Charge covering the area where the mail cover is to be placed.

(2) This airtel 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) Upon FBIHQ approval, 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, FBIHQ approval must be obtained prior to submitting the request for extension to the appropriate USPS authority. Any request for FBIHQ approval for extension beyond 120 days must clearly set forth the specific reasonable grounds that exist which demonstrate the mail cover is necessary.

(5) In 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. In these situations, FBIHQ authority may be obtained by telephone, followed by confirming teletype or by immediate teletype requesting emergency authority to establish a mail cover. As in routine instances, FBIHQ approval must be obtained prior to making an emergency request to the Postal Inspector in Charge for a mail cover. Emergency requests must also set forth the same information as that which is required in routine requests.

EFFECTIVE: 05/10/82

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
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

10-7.2 Placement of Stops

b2
7E

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.

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

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

b2
7E

10-7.5.1 [redacted]

Stop notices are placed by letter to [redacted]

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

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] 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" (NAILS), 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] b7E Per INS

(a) [redacted]

(b) [redacted]

(c) [redacted]

(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

b2
7E

10-7.5.3 [redacted]

[redacted]

(1) [redacted]

[redacted]

b2
7E

(2) [redacted]

(3) [redacted]

EFFECTIVE: 02/16/89

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

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 a finding that the records are relevant to a legitimate law enforcement inquiry (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 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 Legal Research Unit, FBIHQ.

EFFECTIVE: 01/22/90

10-8.2 Access to Transactional Information

(1) Telephone Toll Records

(a) Criminal and Civil Matters - Access to telephone toll records is governed by Title 18, USC, Section 2703. Specifically, the disclosure of toll records to a governmental entity is permitted only when the governmental entity:

1. uses an administrative subpoena authorized by a Federal or state statute, or a Federal or state grand jury|or trial|subpoena;

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

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

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

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 toll 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 toll 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, Part I, Section O.

(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) Subscriber Listing Information

Criminal and Civil Matters - Some telephone companies are requiring compliance with Title 18, USC, Section 2703 before they will release subscriber listing information, including that which is publicly available. It is the opinion of the Department of Justice that Title 18, USC, Section 2703(c) was not intended to apply to subscriber information, whether published or unpublished. Questions concerning this issue should be directed to the Legal Research Unit, FBIHQ.

(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 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: 01/22/90

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

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 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. 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

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] 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.

b2

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 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

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

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 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 overhear 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 overhear will not be prematurely disclosed to the requester.

(5) Therefore, in responding to an FOIPA Section airtel

another office.

EFFECTIVE: 12/10/93

10-9.8 Preservation of Original Tape Recordings

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 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: 08/12/86

10-9.8.1 FD-504 (Chain of Custody - Original Tape Recording Envelope)

(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, exhibited as a bulky 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 (Bulky Exhibit) 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.

(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 a bulky exhibit within five days of the receipt of the recording, as required in the Manual of Administrative Operations and Procedures, Part II, Section 2-4.4.1(1)(b). All original tapes are to remain in the field office where first entered as a bulky exhibit. 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 bulky exhibits, 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: 08/12/86

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.

EFFECTIVE: 10/18/88

10-9.10 Electronic|Surveillance| - Title III Criminal Matters
|(See MIOG, Part II, 10-3, 10-9.1(6) & 10-10.9.1(8)(c).)|

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, kidnaping, robbery or extortion prosecutable under Title 18, U.S. Code;

(c) Presidential assassination, kidnaping, 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).)|

(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 Foreign Counterintelligence Manual, Part I, 0-2.6.3 & Appendix 10, 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 principal legal advisor (PLA) and the concurrence of the respective USA or Strike Force Attorney. The PLA 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 review of an electronic surveillance request is a three-fold operation: case supervision, legal analysis and executive approval. In this regard, those applications involving the following sensitive issues or circumstances require the approval of the Director or Acting Director:

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

2. 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);

3. 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;

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

5. situations involving significant privacy

concerns (e.g., interceptions of conversations in a bedroom or bathroom, etc.);

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

7. in any other situation deemed appropriate by either the Assistant Director, Criminal Investigative Division, or Legal Counsel Division, or their Deputies.

Nonsensitive Title III applications for electronic surveillance of wire and oral communications and of electronic communications not involving [redacted] may be approved by the Assistant Director or Deputy Assistant Director acting on his/her behalf in the Criminal Investigative Division. Legal Counsel Division will review and approve all such Title III submissions prior to final executive approval.

b2
7E

Title III applications for authorization to intercept electronic communications over a [redacted] do not require FBIHQ review and approval, but may proceed with SAC approval. |(See MIOG, Part II, 10-10.11.1(2)(b).)|

(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 airtel 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.|

(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;

b2
7E

(d) That minimization will be assured, especially when the coverage involves a [redacted] 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 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 airtel 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 Interceptees;

(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.

(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 a memorandum, airtel, 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 Unit 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 10-10.9 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 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 [redacted] 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)).

b2
7E

(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 [redacted] (Title 18, USC, Section 2518(11)(b)). b2 7E

(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 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 [redacted] 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. b2 7E

(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.

(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 origiral 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.

EFFECTIVE: 10/15/93

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

"(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) A field office seeking emergency Title III authorization should telephone such request, along with all known facts and circumstances, to the Criminal Investigative Division (CID), FBIHQ. During weekend, holiday, or nighttime hours requesting field offices should telephone the request to the CID Duty Supervisor. In either case the telephone request should be followed by a teletype setting forth details contained in the telephone request.

(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 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 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 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. However, for purposes of administrative control, DOJ continues to require that prior approval for such interceptions be obtained in the same manner currently required for the approval of consensual monitoring of nontelephone oral communications (body recorders and/or transmitters), that is by obtaining emergency FBIHQ authority which is thereafter confirmed in writing to DOJ. These procedures entail consultation with and concurrence of a representative of the local USA's office, followed by a request to FBIHQ for emergency authority. The request and the basis for same are thereafter confirmed in writing with the DOJ. (See 10-10 for detailed requirements.) 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 Principal Legal Advisor.) CID will furnish all known facts and recommendations to Legal Counsel Division (LCD), which will make the final determination regarding the presence or absence of a justifiable expectation of privacy. If LCD 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 LCD with respect to the absence of a justifiable expectation of privacy and the basis for that conclusion. If LCD determines that a justifiable expectation of privacy does exist, Title III authority is of course necessary for the microphone 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] 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. Requests for authorization to utilize such devices in ransom packages should be telephoned to the appropriate substantive desk at FBIHQ.

b2
7E

(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. LCD 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: 04/24/89

||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 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 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 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 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).

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.

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 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.

(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 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 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
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

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.
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

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-2
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 facility.

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

1. Proprietary Interest card for filing by name.

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

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
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 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

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, 2-4.4.10(1).

EFFECTIVE: 04/19/91

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 conversation 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 conversation 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.

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

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

EFFECTIVE: 04/19/91

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 nonsensitive criminal matters. This authorization should be in writing, 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, 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 Agents 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-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 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;

(b) |Prior to its initial use, the USA, AUSA, or Strike Force Attorney in the district where the monitoring will take place 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(10).)|

(c) Separate control files -- for body recorders and/or transmitting devices and another 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. These control files will be for the purpose of the SAC's administrative control and for review during inspection.

(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: 10/15/93

10-10.3 Monitoring Nontelephone Conversations 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.|

(1) On 11/7/83, the Attorney General issued "Procedures for Lawful, Warrantless Interceptions of Verbal Communications." The guidelines supersede those issued by the Attorney General on 9/22/80. They apply to all nontelephonic consensual monitoring in criminal investigations. All requests, except those in which one or more of seven listed circumstances are present, can be approved at FBIHQ or, where an emergency situation exists, by the SAC, as opposed to the Department of Justice (DOJ). |(See MIOG, Part II, 10-10.3 (3) & (8).)| These seven circumstances requiring DOJ approval 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 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 (8):

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

||(See MIOG, Part II, 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 Principal Legal Advisor prior to submission of the communication to FBIHQ with the name of the Principal Legal Advisor 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 designated Criminal Investigative Division Section Chiefs or their next superior officials as FBIHQ officials who can approve those consensual monitoring requests which do not require DOJ approval. Where emergency situations exist, consensual monitoring authority may be granted by the respective SAC. | (See|(1) &|(8).)

(4) In view of these regulations, when it is anticipated that nontelephone consensual monitoring will be used, authority through FBIHQ must be obtained. This request should reach FBIHQ at least seven calendar days prior to its anticipated use. Agents should continue to obtain written consent, as documented by an executed Form FD-473, 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 Special Agents 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-473. This form should then be executed in all respects with the exception of the consenting party's signature. ||(See MIOG, Part II, 10-10.9.1(6).)|

(5) 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 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.

(6) No exception should be made to executing and properly witnessing the consent form in the situation where an informant, a Special Agent or any other law enforcement 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).

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

(8) In requesting FBIHQ authority for use of nontelephone monitoring equipment in nonemergency situations, 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), & (3) above.)|

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

DETAILS: Begin with a sentence which states whether or not this request requires DOJ approval. If DOJ approval is required, identify which of the seven sets of circumstances require such approval and provide a statement that the Principal Legal Advisor, identified by

name, has reviewed and approved the communication for legal sufficiency. Describe background of case--reasons why device is needed and when and where needed. Identify person who is to wear device or indicate if fixed device is to be used (body recorder, transmitter, 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 informant, person whose identity should be protected, or undercover Agent is consenting party, identify person as "source." Show under Administrative Data the symbol number of informant, identity of undercover Agent, or name of person whose identity is to be protected. Show 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 Special Agents.

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.

EMERGENCY AUTHORITY: If circumstances of an exigent nature arise which preclude a routine request, authority for the use of nontelephone consensual monitoring equipment may be granted by the SAC of the respective field division. In each instance where emergency authority has been granted by the SAC, Form FD-759 must be executed by the field office and forwarded to FBIHQ no later than five working days from the date the authority was granted.

The Attorney General's Guidelines regarding Procedures for Lawful Warrantless Interceptions of Verbal Communications (see 10-10.3(1)) cite seven sensitive situations which require written authorization from the DOJ for approval. 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, subsequent DOJ notification is required and will be handled by FBIHQ upon receipt of Form FD-759.

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.

(9) 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 FBIHQ and/or DOJ authorization. If it is

anticipated that an extension of authority will be needed, ensure that the requesting teletype is received at FBIHQ at least seven days prior to expiration of authority. Authority is granted for a period of 30 days on each request. Within 30 days of the expiration of authorization and each extension thereof, an FD-621 shall be prepared under the substantive case caption including the character of the case, executed in its entirety and forwarded to FBIHQ in a sealed brown envelope labeled "Director, FBI, ELSUR Index, FBIHQ."

(10) |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: 10/15/93

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 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

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.

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 exhibit 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 number is to be set forth on the FD-192 (Bulky Exhibit-Inventory of Property Acquired as 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 appropriate section 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 the appropriate section of the Foreign Counterintelligence Manual.

EFFECTIVE: 12/20/93

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 & 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) 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 legal advisor 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.

(3) 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.

(4) 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 "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.

(5) 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: 12/14/93

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 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 not be obtained.

EFFECTIVE: 01/22/90

10-10.8 Electronic Tracking Devices

b2
7E

Electronic tracking devices [redacted] are called beepers. The two devices must be distinguished from each other. This section addresses electronic tracking devices. [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

(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, FBIHQ authorization is required before such a device is utilized.

EFFECTIVE: 01/22/90

10-10.9 Closed Circuit Television (CCTV) (Video Only) - Criminal Matters

(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 (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 implementation.

(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: 01/22/90

10-10.9.1 CCTV Authorization Delegated to Bureau Officials - Criminal Matters |(See MIOG, Part I, 9-7.2.)|

(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) Authorization by SAC - The SAC of the Bureau field office in whose territory the monitoring is to occur may authorize for a period of up to 30 days, unless otherwise specified, the use of CCTV where:

(a) the area to be viewed is an exterior public area, such as a public street or an exterior door, and

b2
7E

(b) the camera is located in a public area or is placed in a location under the exclusive possession and control of the FBI, [redacted]

The SAC will consult with the field office Principal Legal Advisor and the United States Attorney (USA) in all cases in which questions or sensitive or unusual circumstances arise. (The opinion of the USA, if required, is to be confirmed in writing, if not obtained in writing.)

(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 substantive case file, with a copy designated for the field office control file. Form FD-677 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) Authorization by Designated FBIHQ Officials - The Section Chief of the appropriate section of the Criminal Investigative Division (CID), FBIHQ, may authorize for a period of up to 30 days, unless otherwise specified, the use of CCTV where:

(a) the area to be viewed is an interior common area, such as a public hallway in a building or the lobby of an apartment building, motel or bank; and

(b) the camera is located in a public area, or area under the exclusive possession and control of the FBI; or

(c) the 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 within a possessory interest in the premises.

The Section Chief will consult with the Legal Counsel Division (LCD) where any questions or unusual circumstances arise.

(5) Authorization by the DOJ - In situations where no court order is required, DOJ authorization for a period of up to 30 days, unless otherwise specified (obtained via appropriate communication to the CID, FBIHQ), is required for the use of CCTV to view the interior of private premises or other areas where a reasonable expectation of privacy otherwise exists, but a participant in the activity to be viewed has consented to such monitoring. In any

situation where there is uncertainty as to the existence of a reasonable expectation of privacy, DOJ authority must be sought. All requests requiring DOJ approval shall be reviewed and approved by the Principal Legal Advisor prior to submission of the communication to FBIHQ.

(6) Nonemergency requests of the DOJ for authorization of CCTV surveillance will follow the same authorization procedures and rules as used in nontelephone consensual monitoring requests. Review MIOG, Part II, Section 10-10.3 (4), et seq.

(7) "Emergency" Authorization - In those unique situations where CCTV surveillance requests cannot be delivered to the DOJ at least 48 hours before the proposed use, the appropriate CID Section Chief, with the concurrence of the Principal Legal Advisor, may furnish "emergency" authorization for the use of CCTV, if, in their judgment, judicial authorization is not required. In such cases, the Section Chief must give written notice to the DOJ no later than five working days after such emergency authorization is given. This notification shall set forth the nature of the emergency; the need for expeditious action; and a description of the investigation being conducted, including the subject of the investigation and the method of utilization of CCTV surveillance. In order for this deadline to be met, it will be necessary for field offices telephonically receiving emergency authorization to submit to the substantive unit at FBIHQ a teletype setting forth appropriate details within two working days of the granting of such authorization. (Refer to paragraph (10) below.)

(8) Judicial Authorization - Judicial authorization, after DOJ approval, is required for the use of CCTV in all cases 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. This requirement includes the situations where CCTV is to be used in conjunction with such court-ordered aural surveillance under Title III, even if it is to be used only for minimization purposes. Where CCTV is to be used in conjunction with such court-ordered aural surveillance, judicial authorization will be initiated by:

(a) A separate section of the Title III affidavit establishing probable cause that the activity to be surveilled will, in fact, be acquired; the proposed location of the camera; names of persons expected to be viewed; and a statement made by the affiant that in the affiant's judgment, the video surveillance is warranted; and

(b) A separate application and draft order prepared by the appropriate United States Attorney for the video surveillance, in addition to the usual application and order for aural surveillance.

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

(9) Documentation of Consent - In those situations requiring the consent of an individual for either the monitoring or the placing of the equipment, Agents should obtain written consent 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 Agents should be present to witness this consent, and the fact that the consenting party has declined to give written consent should be appropriately documented and witnessed. No exceptions should be made to executing and properly witnessing this consent in a situation wherein an informant, a cooperating witness, a Special Agent, or any other law enforcement officer is the consenting party.

(10) In requesting FBIHQ/DOJ authority for the use of CCTV equipment, an appropriate communication is to be submitted under the substantive case caption and directed to the appropriate section of the CID, FBIHQ. Only in the Administrative Data portion of this communication should the consenting party be identified (if protection is sought) by symbol number or name. It should be noted that if DOJ authorization is being sought, a copy of the field communication may be forwarded from FBIHQ directly to the DOJ along with the request, excising from the communication the "ADMINISTRATIVE DATA" portion. It will be necessary to use the following format in the field communication: (See (7) above.)

PURPOSE: Authority is requested to conduct a Closed Circuit Television Surveillance in connection with a _____(character)_____ matter.

LOCATION: (Identify: --

(a) the specific area to be subjected to CCTV surveillance, noting if the surveillance is an interior common space, or if the surveillance is to be conducted with the consent of a participant in the activity to be viewed, and

(b) the specific location where the camera is to be placed, noting how access to such location is to be achieved. If

access is to be given with the consent of a person with a possessory interest in the premises, state such consent has been obtained.)

DETAILS: (Begin with a sentence which states whether or not the request requires DOJ approval and the reason for such and provide a statement that the Principal Legal Advisor, identified by name, has reviewed and approved the communication for legal sufficiency. Briefly provide a description of the investigation being conducted, identifying the subject of the investigation and the anticipated target(s) of the surveillance. Set forth the method of utilization of the CCTV surveillance, if not fully described above. If utilization is to be dependent upon the consent of a participant in the activity to be viewed, indicate that this person has granted consent and has agreed to testify, if required, and that the device will only be used when the consenting party is present. If an informant, a person whose identity should be protected, or an undercover Agent (UCA) is the consenting party, identify this person as "source." Show under "ADMINISTRATIVE DATA" the symbol number of the informant, the identity of the UCA, or the name of the person whose identity is to be protected.)

EMERGENCY AUTHORITY (if necessary): (If emergency authority is being requested in a teletype, describe the nature of the emergency and the need for expeditious action.)

(If emergency authority was granted telephonically by an FBIHQ official, use the following phrase:

"Emergency authorization was granted by an FBIHQ official because... (describe the nature of the emergency and the need for expeditious action)")

(In instances where emergency authorization is telephonically provided to a field office, a record is to be made in the field office file of the date, the name of the individual furnishing such authorization, and the name of the individual to whom it was provided.)

ADMINISTRATIVE DATA: (All administrative data, including symbol number of informant, identities of UCAs, or names of persons to be protected, should be set forth in this section.)

(11) 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.

(12) All offices should ensure appropriate administrative controls are established. If it is anticipated that an extension of authority will be needed, ensure that the requesting teletype is received at FBIHQ at least seven days prior to expiration of authority.

EFFECTIVE: 10/15/93

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 conversations, but requires the additional information noted under the subheading "LOCATION" in (10) above. See also Part II, Section 10-10.3 of this manual entitled "Monitoring Nontelephone Conversations in Criminal Matters.")

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

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

EFFECTIVE: 07/18/86

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 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

b2
7E

10-10.11.1 [redacted]

[redacted]

(1) [redacted]

(a) [redacted]

4-750 (Rev. 12-14-88)

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 you or the subject of your request.

☐ Information pertained only to a third party. Your name 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 for the following reason(s): _____

☐ For your information: _____

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

MIOG, Part II, Section 10, page 90

XXXXXX
XXXXXX
XXXXXX

XXXXXXXXXXXXXXXXXXXXXX
X DELETED PAGE(S) X
X NO DUPLICATION FEE X
X FOR THIS PAGE X
XXXXXXXXXXXXXXXXXXXXXX

FBI/DOJ

b2

[redacted] ELSUR indexing is required.

EFFECTIVE: 06/26/91

10-10.11.2 Other Types of Radio Monitoring

(1) The radio portion of handheld or cordless telephone conversations are specifically excluded from Title III requirements (Title 18, USC, Section 2510(12)(A)). These devices utilize a radio transmission over a limited distance to a base station at a regular telephone. They are so easily intercepted, often over an ordinary AM radio, that there is no reasonable expectation of privacy in these communications.

(2) Other radio communications such as those that are broadcast so as to be readily accessible to the public (AM and FM radio station broadcasts), ship to shore general public type communications, public safety communications, citizen band amateur and general mobile radio services, and the like are also specifically excluded from Title III requirements (Title 18, USC, Section 2511(2)(g)).

(3) No judicial warrant of any type is required for the interception of the radio communications set forth above. SACs may authorize such interceptions. ELSUR indexing is not required. Interceptions should be logged and reported on FD-302s.

(4) Certain hybrid communications which contain both wire and radio components such as cellular telephones (both wire and radio portion) are covered by Title III, whereas others are not, e.g., cordless telephones (radio portion not covered). Any question regarding whether a particular device or radio communication is covered by Title III should be directed to the Legal Research Unit, FBIHQ.

EFFECTIVE: 10/18/88

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.

EFFECTIVE: 10/18/88

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.

b2
7E

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

EFFECTIVE: 10/18/88

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

10-10.16 [redacted]

b2
7E

(1) [redacted]

(2) [redacted]

(3) [redacted]

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

(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

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.

b2
7E

(6) Further details as to [redacted]

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) 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.

(5) 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.|

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

(7) 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; field offices should not routinely request a trap and trace and should limit the utilization of this technique to only those situations where it is absolutely necessary.

(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.

(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: 12/14/93

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

(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.

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|

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|

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

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, who may delegate this authority to the Section Chief level. The Behavioral Science Instruction and Research Unit, Training Division, 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 expert's qualifications. You should consider utilizing only a psychiatrist, psychologist, physician, or dentist who is qualified as a hypnotist. Upon receipt of Bureau authority, the matter must be thoroughly discussed with the USA or Strike Force Attorney in Charge, including the fact that a specially trained Agent (hypnosis coordinator) will participate in the hypnotic session. The USA or Strike Force Attorney In Charge is to be advised that he/she must obtain written authorization of the Director or the Associate Director, Office of Enforcement Operations, Criminal Division, in each case. You are cautioned that under no circumstances will Bureau personnel participate in hypnotic interviews in non-Bureau cases.

EFFECTIVE: 02/16/89

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 the Hypnosis Coordinator

The hypnotic session should be attended by the hypnotist and the specially trained Bureau Agent (hypnosis coordinator) who will act as liaison with the hypnotist. It must be clearly understood that the hypnotist is charged with the responsibility of supervising the hypnotic session and must remain physically present throughout the proceedings. The hypnosis coordinator is qualified to question the witness or victim while under 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 Bureau hypnosis coordinator who is acting as liaison.

The Agent assigned to the case may also be present at the interview if there are no objections by the hypnotist; however, the number of persons actually present at the hypnotic session should be held to a minimum.

EFFECTIVE: 11/20/90

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 Training Division. 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 hypnosis coordinator and the hypnotist.

(5) Disposition of the case.

EFFECTIVE: 11/20/90

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

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

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 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.

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

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 Part I, Section 0-4 of the Foreign Counterintelligence Manual.

EFFECTIVE: 12/07/93

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.

b2
7E

(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.

(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.

b2
7E

(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.

(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.

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.

b2
7E

(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:

(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) & 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.

(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:

b2

Department of the Treasury - Federal Reserve Bank,
New York City, Treasury Department Code [redacted]
for credit to [redacted]

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 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

4-750 (Rev. 12-14-88)

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 you or the subject of your request.

☐ Information pertained only to a third party. Your name 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 for the following reason(s): _____

☐ For your information: _____

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

MIOG, Part II, Section 10, page 114

XXXXXX
XXXXXX
XXXXXX

XXXXXXXXXXXXXXXXXXXXXX
X DELETED PAGE(S) X
X NO DUPLICATION FEE X
X FOR THIS PAGE X
XXXXXXXXXXXXXXXXXXXXXX

FBI/DOJ

b2

11-4.7.3 Publicity

[redacted]

11-4.8 Miscellaneous

[redacted]

11-4.9 Photograph of Subjects

[redacted]

[[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 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.]

SECTION 12. FIREARMS

EFFECTIVE:

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

In 1934, Congress authorized Special Agents (SAs) of the Federal Bureau of Investigation to carry firearms under Title 18, USC, Section 3052.

EFFECTIVE: 05/20/94

12-1.1 SAC Responsibility

SACs are ultimately responsible for the use and maintenance of all firearms and related equipment in their respective divisions, including training. SACs are also responsible for all defensive tactics training and related equipment. A Principal Firearms Instructor (PFI) will be assigned by the SAC to manage the division firearms program. A primary defensive tactics instructor (PDTI) will be assigned by the SAC to manage the Defensive Tactics Program.

EFFECTIVE: 05/20/94

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

SAs are directly responsible for all aspects of the use and maintenance of firearms and related equipment under their control. Firearms instructors will be trained by the FBI Academy, Firearms Training Unit (FTU), and defensive tactics instructors trained by the FBI Academy, Physical Training Unit (PTU), to support the Field Firearms and Defensive Tactics Programs. [redacted] b2 b7E

EFFECTIVE: 05/20/94

12-2 |UTILIZATION OF FIREARMS|

EFFECTIVE: 05/20/94

12-2.1 |Policy|

EFFECTIVE: 05/20/94

12-2.1.1 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.)

(1) Policy Text - "Agents are not to use deadly force against any person except as necessary in self-defense or the defense of another, when they have reason to believe they or another are in danger of death or grievous bodily harm."

(2) Definitions

(a) Deadly force - Force that is likely to cause death or serious bodily injury.

(b) Reasonable grounds to believe - facts that would cause a reasonable person to conclude that the point at issue is probably true (Probable Cause).

(c) Necessary - Alternative steps are not likely to lead to safe control of the subject.

(3) Required Showing to Justify Use

(a) Individual was likely to cause death or serious bodily injury if not controlled, AND

(b) Deadly force was necessary to safely achieve control.

(4) Assessing Dangerousness

(a) Reasonably believed to previously have caused or attempted to cause death or serious bodily injury to Agents or other persons; or

(b) Reasonably believed to be armed with a deadly weapon; or

(c) Not reasonably believed to be armed but

reasonably believed to be presently arming self with deadly weapon; or

(d) Not reasonably believed to be armed but reasonably believed to have the ability to inflict serious injury without the use of a deadly weapon and to be resisting; or

(e) "Armed and Dangerous" notation, standing alone, is insufficient.

(5) Assessing Necessity

(a) Policy statement: "Whenever feasible, verbal warnings should be given before deadly force is applied."

(b) Where a subject may be granted an opportunity to surrender without exposing Agents or the public to unreasonable danger, policy requires that the opportunity be given.

(c) Considerations:

1. The likelihood that the person will resist

2. The person's actions when confronted

a. noncompliance

b. resistance

3. The person's known and likely capabilities

(d) Factors:

1. Availability of cover

2. Persons in vicinity at risk

3. Likelihood that subject will surrender

4. Nature of threat posed

(6) Degree of Force Permitted

(a) Reasonable force

1. Where deadly force is permissible, Agents may utilize the amount of force reasonably necessary to eliminate the threat they are facing

a. if shooting in self-defense or defense of others, they may fire until the subject surrenders or no longer poses a threat

(7) Judicious Application of Deadly Force

(a) Sound judgment still required

1. Where deadly force is permissible under FBI policy, Agents still have the duty to assess whether their use of deadly force creates a danger to the public that outweighs the likely benefit of that use of force.

(8) Warning Shots

(a) Policy Text: "No warning shots are to be fired by Agents..."

(b) Justification: Warning shots are forbidden because firing a gun creates the potential for unintended injury.

EFFECTIVE: 05/20/94

12-2.1.2 Carrying of Weapons

(1) SAs must be armed or have immediate access to a firearm at all times when on official duty unless good judgment dictates otherwise. SAs are authorized to be armed when off-duty.

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

(3) Safety levers should not be engaged on any pistol constructed with a double action first shot. With the exception of single-action pistols, handguns should not be carried in a cocked mode.

(4) When an SA is moving, the finger must be off the trigger, double-action weapons should be decocked and safety engaged on single-action weapons, unless exigent circumstances are present.

(5) To preclude unintentional discharges when covering an adversary, double-action weapons should be decocked and single-action weapons (including shoulder weapons) should either have the safety

engaged or finger off the trigger, unless exigent circumstances are present.

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

(7) Unless operationally deployed, shoulder weapons should be maintained with no round in the chamber.

(8) 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.

(9) SAs must be familiar with and currently qualified with all firearms and equipment they carry and are personally responsible for appropriate use, security, and maintenance of these firearms.

(10) 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 so that they have no opportunity to either resist or flee.

(11) SAs may draw their weapons without being confronted with a deadly force situation if good judgment dictates or in exigent circumstances. Proper training and experience in arrest situations must be relied upon to provide the proper response when confronted with deadly force situations.

(12) Handguns should be carried on the SA's person.

(13) SAs should avoid unnecessary display of weapons in public. Good judgment must dictate in all situations.

(14) Accidental or unintentional discharge of a weapon is extremely dangerous to the public and to FBI personnel and will not be tolerated. Any unintentional discharge must be reported to FBIHQ using FD-418.

(15) Specialized weapons, i.e., M-16, MP5A3, gas delivery systems, etc., must only be deployed by SAs trained and currently qualified in their use.

EFFECTIVE: 05/20/94

12-2.1.3 Firearms Aboard Aircraft (See MIOG, Part I, 164-15 (4).)

(1) Title 49, USC, Section 1472(1), generally forbids carrying firearms aboard aircraft. SAs 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) FBI SAs are instructed to carry a firearm on their person aboard any commercial domestic flight when on official business, unless operational considerations dictate otherwise.

(4) SAs must avoid unnecessary display of firearms to the public while traveling by aircraft.

(5) The FBI has exclusive jurisdiction over the Aircraft Piracy Statute, interference with flight crew and certain crimes aboard aircraft.

EFFECTIVE: 05/20/94

12-3 ISSUED WEAPONS

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

(2) A handgun, 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. Unless operational needs dictate otherwise, handguns should be sighted in for [redacted] b2 b7E

(5) Any changes or alterations to any assigned weapon must be authorized by the Firearms Training Unit (FTU).

EFFECTIVE: 05/20/94

12-3.1 Distribution of Firearms

Depending on operational considerations, each field office must maintain an adequate number and type of firearms.

(1) Handguns -

(a) SAs are permitted to have a total of three assigned handguns in any combination of revolvers and semiautomatic pistols. This includes Bureau-issued handguns. SAs may elect three personally owned weapons, but must then turn in the Bureau-issued handgun. Current Bureau firearms instructors are exempted from this requirement.

(b) Handguns are intended for general self-defense and should not be solely relied upon for offensive operations, e.g., raids, arrests.

(c) The Bureau is equipped with Smith and Wesson revolvers.

(d) Small-framed revolvers, i.e., M-36, M-49, M-60, etc., are intended for use when concealability is important.

(e) Maximum range is defined as that greatest distance a bullet will travel when fired from a particular weapon. "Effective" range is defined as the greatest distance from which a competent shooter could reasonably expect to accurately hit a target. Maximum and effective ranges of approved revolver ammunition are listed below:

CALIBER	MAXIMUM RANGE	EFFECTIVE RANGE
.38 Special (147 gr.)	1800 yds.	[redacted]
.357 Magnum (158 gr.)	2700 yds.	

b2
b7E

(f) The Bureau is equipped with Smith and Wesson, Browning Hi-Power and Sig Sauer semiautomatic pistols.

(g) Maximum and effective ranges for pistol ammunition are listed below:

CALIBER	MAXIMUM RANGE	EFFECTIVE RANGE

b2
b7E

9mm (147 gr.)	1800 yds.	[redacted]
10mm (180 gr.)	2166 yds.	
45 cal (230 gr.)	1466 yds.	

(2) Shotguns

(a) The Bureau is equipped with Remington Model 870 12-gauge shotguns with 14, 18 and 20-inch barrels.

(b) Maximum and effective ranges for shotgun ammunition are listed below:

AMMUNITION	MAXIMUM RANGE	EFFECTIVE RANGE
00 Buck (9 pellet)	500 yds.	[redacted]
Rifled Slug (1 oz.)	900 yds.	

b2
b7E

(3) Rifles

(a) The Bureau is equipped with the following rifles:

MODEL	CALIBER
Winchester 70	30.06 Springfield (S)
Winchester 70 (custom heavy barrel)	.308 Winchester (W)/7.62mm
Remington 700 (heavy barrel)	.223 Remington (R) or 308 (W)
Colt M-16A1 (rifle and carbine)	.223/5.56mm
Colt M-16A2 (rifle and carbine)	.223/5.56mm

(b) Bolt action and fully automatic rifles are authorized for use only by current firearms instructors, [redacted] who are qualified. (Any exception to this requirement must be approved by the Unit Chief, FTU.)

b2
b7E

(c) Weapons capable of fully automatic or "burst" fire, e.g., M16A1 and M16A2 rifles (some weapons may be equipped with selector locks designed to function in semiautomatic mode only) may only be used by current firearms instructors, [redacted] who are currently qualified in their use. Any other SA can use these weapons if equipped with a fire selector lock and are qualified in their use.

b2
b7E

(d) The SAC has the authority during emergency situations to approve removal of the selector locks on M16A1 or M16A2 rifles. This authority may not be delegated and should only be exercised during the most exigent circumstances. This weapon should

then only be issued to personnel such as [redacted] or Bureau-trained firearms instructors who are qualified. Upon termination of the emergency situation the SAC must ensure the selector locks are properly reattached to the weapons [redacted] b2 b7E

(e) Bureau rifles should be sighted in during firearms training sessions to ensure accuracy.

(f) Maximum and effective ranges for approved rifle ammunition are listed below. [redacted] b2 b7E

CALIBER	MAXIMUM RANGE	EFFECTIVE RANGE
.223 R (55/69 gr.)	2900 yds	[redacted]
.308 W (168 gr.)	5500 yds	
30.06S (150 gr.)	5500 yds	

b2 b7E

(4) Submachine Guns

(a) The Bureau is equipped with Heckler and Koch submachine guns.

(b) Submachine guns may only be used by current firearms instructors, [redacted] who are currently qualified in their use. b2 b7E

(c) The Thompson submachine gun may only be used for display and demonstration purposes.

(d) Maximum and effective ranges for submachine gun ammunition are listed below:

CALIBER	MAXIMUM RANGE	EFFECTIVE RANGE
9mm (147 gr.)	1900 yds	[redacted]
.45 ACP (230 gr.)	1760 yds	

b2 b7E

(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 provided they are currently qualified with the weapon.

(c) The M16A1 and M16A2 carbines are authorized for use only by currently qualified firearms instructors, [redacted] unless equipped with fire selector locks. [redacted] b2 b7E

(d) Maximum and effective ranges of carbine ammunition are listed below:

CALIBER	MAXIMUM RANGE	EFFECTIVE RANGE
9mm (147 gr.)	1900 yds	[redacted]
.223R (55/69 gr.)	2900 yds	

b2 b7E

EFFECTIVE: 05/20/94

12-4 PERSONALLY OWNED WEAPONS

EFFECTIVE: 05/20/94

12-4.1 Policy

(1) SAs are authorized to carry approved personally owned weapons (POWs) in lieu of a Bureau-issued firearm, provided the SA is currently qualified with those weapons.

(2) SAs are authorized one Remington Model 870 shotgun with barrel length of no more than 20 inches and no less than 18 inches provided the SA is currently qualified to use that weapon. A personally owned shotgun must have a "flexi-tab" shell carrier installed by the Quantico Gun Vault.

(3) SAs are authorized one AR-15 rifle or carbine or one Heckler and Koch Model 94 provided the SA is currently qualified with that weapon.

(4) Before approval of a POW is granted, the weapon must be inspected by the Principal Firearms Instructor (or designee) for condition, serviceability, and required features before submission to the FBI Academy Gun Vault for inspection.

(5) 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.

(6) POWs authorized to be carried on official business are to be treated in the same manner as nonexpendable Bureau property.

(7) No firearm will be approved as personally owned 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:

(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.

(8) Only revolvers of the type issued by the FBI are approvable. In order to be approved, the revolver must be chambered for .38 Special or .357 Magnum, have a blued or stainless steel finish, steel frame, barrel length no shorter than two inches and no longer than four inches, and hold a minimum of five cartridges. A current list of approvable revolvers is maintained by the Firearms Training Unit (FTU) and Gun Vault.

(9) Only semiautomatic pistols of the type and caliber issued by the FBI are approvable. The prospective POW must have an approvable factory finish, have an all steel or aluminum alloy frame with a barrel length not to exceed five inches. A current list of approvable pistols is maintained by the FTU and Gun Vault.

(10) Authority to carry any other pistol must be granted only by the FTU or, in the case of specialty weapons, by the Criminal Investigative Division on a special case basis.

(11) Pistols must be equipped with a minimum of four magazines.

(12) 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 may be withdrawn.

(13) Shotguns with magazine extensions or collapsible stocks will not be approved.

(14) Approval Procedure

(a) The field division PFI will manage this program for the office.

(b) A SA seeking weapon approval will submit FD-431 in quadruplicate to PFI with the weapon for approval.

(c) PFI (or firearms instructor) will verify that the weapon meets the requirements for approval as a POW in terms of condition, serviceability, required features, and being an approvable model.

(d) PFI (or firearms instructor), after signing the FD-431, will submit the forms for SAC approval and transmittal, returning three copies of the FD-431 to FBI Academy Gun Vault WITH THE WEAPON. One copy of the FD-431 should be maintained as a field office tickler copy. Pistols must be accompanied by four factory magazines and magazine-fed shoulder weapons must be submitted with a minimum of two factory magazines.

(e) Weapons must be clean, unloaded, properly packaged, and properly shipped.

(f) Gun Vault will inspect for physical condition and test fire the weapon for functionability.

(g) 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.

(h) 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.

(i) 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.

(j) Any reason for disapproval of a weapon will be explained in full on the FD-431 and with the weapon returned to the submitter.

(15) 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, enter deletion on SAs firearms training records.

(16) Any questions regarding approval of any POW should be resolved with the FTU prior to purchase or request for approval.

EFFECTIVE: 05/20/94

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 approved by the Firearms Training Unit (FTU) in advance.

(3) After-market parts or options are not approved unless authority is granted by FTU policy. Nonstandard factory parts must also be approved by the FTU.

(4) SAs are to bring all Bureau-assigned handguns to the Gun Vault each time they attend an in-service or conference at the FBI Academy.

(5) [redacted] b2 b7E

(6) 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.).

(7) Any violations of above policy must be reported via airtel to FBIHQ and the FTU for possible administrative action.

(8) Firearms must be unloaded, cleaned, and properly packaged before shipment via Federal Express, or other appropriate means. A cover airtel should be included which states the reason the firearm is being returned to the FBI Academy, Room 110, Building 9, Quantico, Virginia 22135. (DO NOT MAIL WEAPONS "ATTENTION: GUN VAULT"). (See MAOP, Part II, 2-2.2.1 (1) & 6-2.3.9.)

(9) When it becomes necessary to render a weapon inoperable during the course of an investigation, it must be accomplished under the direction of the Gun Vault.

(10) Field offices intending to use seized guns for demonstrations or teaching purposes must first submit those weapons to the Gun Vault for inspection, approval, and possible modifications.

EFFECTIVE: 05/20/94

12-5.1 Care of Firearms

(1) After being used and periodically during storage, all weapons should be carefully cleaned and a thin film of oil left in the chamber(s), barrel, and on all exposed metal surfaces to include magazines.

(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.

EFFECTIVE: 05/20/94

12-5.2 Pistol Physical Inspection - (This section is provided as a guide to assist firearms instructors in the thorough examination of pistols for potential damage).

(1) Stress cracks on alloy frames

(a) Inside and outside of rail guides

(b) Slide stop area

(c) All visible pin holes

(d) Take down lever area (Sig Sauer)

(e) Grip (ensure grip does not affect function of magazine release, and decocking lever).

(f) Barrel locking surface

(2) Stress cracks on slides

(a) Inside and outside of ejection port

(b) Recoil guide channel at the muzzle

(c) Slide rail grooves

(d) All visible pin holes

(e) Breech face

(3) Broken parts

(a) Tip of extractor

(b) Ejector

(c) Springs

(d) Recoil guide

(e) Barrel locking surface

(f) Levers

(g) Magazine follower and lips

(h) Magazine welds

(i) Night sights that do not illuminate or missing inserts.

EFFECTIVE: 05/20/94

12-6 SECURITY OF WEAPONS

(1) Each SA is personally responsible for the security of weapons under his/her control.

(2) SACs must provide safe 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) [redacted] 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.

(6) [redacted] 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 - slide closed, hammer released, magazine removed.

(c) Remington Model 870 shotgun - action closed, trigger snapped, safety on.

(d) Colt Model M-16A1/M-16A2 rifles or carbines - magazine removed, action closed, trigger snapped, fire selector on "SEMI."

(e) Winchester Model 70 Rifle - action closed, trigger snapped, safety off.

(f) Thompson submachine gun - magazine removed, action closed, fire selector on "SINGLE," safety on "FIRE."

(g) H&K MP5A3, MP5A3(SD) and MP5-SF - 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: 05/20/94

12-6.1 Security of Weapons at Residence or Non-Government 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.

EFFECTIVE: 05/20/94

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. [redacted]

b2
b7E

(2) [redacted]

(3) Other nonexpendable Bureau equipment related to SA safety may be maintained in the passenger compartment of an unattended Bureau vehicle or vehicle authorized for official use only if properly concealed and if the vehicle doors are 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. This equipment should be stored under the seat whenever possible. If the size of the nonexpendable equipment prevents under-the-seat storage, it is permissible to conceal the item on the floorboard. However, the equipment should not be left on the vehicle seats. Such equipment may be left in this status during any period when operational concerns may require quick access. [redacted]

b2
b7E

(4) Any nonexpendable Bureau equipment not related to SA safety is to be maintained in the locked trunk of an unattended Bureau vehicle or vehicle authorized for official use.

(5) [redacted]

b2
b7E

(6) [redacted]

(7) [redacted]

(8) [redacted]

(9) 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.

EFFECTIVE: 05/20/94

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) During training, any authorized ammunition for FBI use may be fired.

(3) At all other times outside of training sessions, FBI authorized service ammunition must be used.

(4) It is the SAC's responsibility to ensure that the field office maintains an adequate supply of ammunition for training and operational contingencies.

(5) Field office ammunition inventories should be rotated to promote serviceability and be inspected a minimum of once each quarter.

EFFECTIVE: 05/20/94

12-7.1 Training and Service Ammunition

(1) Training ammunition:

(a) .38 Special caliber, midrange wadcutter

(b) All other .38 caliber, 9mm and .45 caliber listed under service ammunition.

(c) 12 gauge #9 skeet shot shell

(d) All other 12-gauge shotgun loads listed under service ammunition.

(e) All carbine and rifle cartridges listed under service ammunition.

(f) 9mm 124 grain full metal case (FMC)

(g) .45 caliber 230 grain FMC

(2) Service ammunition

(a) [redacted]

(b) .357 Magnum Semijacketed hollow point (158g)

b2
b7E

(c) [redacted]

(d) [redacted]

(e) [redacted]

(f) 12 gauge 9 pellet 00 Buck

(g) 12 gauge 12 pellet 00 Buck

(h) 12 gauge 1 oz. Rifled Slug

(i) [redacted]

(j) [redacted]

(k) 30.06 Springfield (150 g)

(l) .223 caliber FMC (55 g)

(m) .223 caliber soft point (SP) (55 g)

(n) .223 caliber HPBT (69 g)

(3) .38 Special caliber ammunition can be fired in a .357 Magnum revolver. Because of a longer cartridge case, a .357 Magnum cannot be fired in a .38 Special revolver.

b2
b7E

(4) For duty use except during firearms training, revolvers must be loaded with .38 Special caliber [redacted]

(5) For justifiable situations when extra penetration or long range are needed from a handgun, .357 magnum revolvers may be loaded with approved .357 magnum ammunition.

(6) .38 Special caliber and .357 magnum ammunition must

not be mixed together in the same revolver. The power of the .357 Magnum could cause the .38 caliber bullet to dislodge from the cartridge case and jam the cylinder.

(7) All ammunition should be stored in a secure, and preferably dehumidified, controlled temperature environment.

(8) Ammunition carried on the person should be used during the next firearms training session and replaced with a fresh supply.

EFFECTIVE: 05/20/94

12-8 FIREARMS PROCUREMENT

(1) The purchase of firearms as Bureau property must be (1) approved by the Firearms Training Unit (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 from the manufacturer for inspection before use.

(3) All Bureau-assigned firearms must be inspected and test-fired by the FBI Academy Gun Vault before use.

(4) Any exceptions to this policy must first be approved by the FTU before procurement.

EFFECTIVE: 05/20/94

12-9 FIREARMS IN RESIDENT AGENCIES

(1) Firearms may be maintained in resident agencies.

(2) All handguns and shoulder fired weapons must be stored in an approved safe, vault or safe-type cabinet.

(3) Whichever storage container is selected, it must be reinforced, fireproof, and have a heavy duty lock or combination dial lock.

(4) Field offices are authorized to purchase safes, vaults, or safe-type cabinets. They must first receive design approval from the Firearms Training Unit (FTU) before pursuing the

procurement process through the Facilities Management Unit (FMU), FBIHQ.

(5) All other conditions sighted herein that govern the use and maintenance of Bureau assigned firearms also apply.

(6) Any exceptions to this policy must be approved in writing by the FTU.

EFFECTIVE: 05/20/94

12-10 FIREARMS TRAINING

(1) The objective of the FBI firearms training program is to annually provide eight (8) opportunities for firearms training. Four (4) of these are mandatory qualification sessions. Field offices whose range availability and ammunition supply will not support this level of training should submit a proposed training plan to the Training Division, Firearms Training Unit (FTU), for approval. This plan should include the number of sessions, courses to be used, and the number of rounds to be fired.

(2) The SAC, through the Principal Firearms Instructor (PFI), is responsible for all firearms training, weapons and ammunition inventories, and overseeing the Field Firearms Program.

(3) SAs and all other personnel authorized to carry firearms must meet or exceed minimum proficiency and safety requirements set forth in the Annual Field Firearms Program.

(4) PFIs are responsible for all transition training either from revolver to pistol or pistol to revolver. The PFI must be satisfied that the 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. PFI must verify this training by documentation on or attached to the SA's FD-40.

(5) Each PFI will strictly adhere to the format of the calendar year Field Firearms Program provided by the FTU. Any changes must be submitted by airtel and approved in advance by the Unit Chief, FTU.

(6) All firearms training sessions must be supervised by the PFI or a Bureau-approved firearms instructor designated by the PFI.

(7) All SAs are required to attend defensive tactics training conducted in conjunction with each of the firearms qualification sessions.

(8) 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 in conjunction with the annual Field Firearms Training Program.

(9) Firearms training requirements are submitted to the field annually by airtel to all SACs, captioned, "Field Firearms Training Program."

(10) Field offices must report the following by airtel captioned, "Annual Field Firearms Training Report," to the FTU by close of business 12/31:

(a) Dates of training sessions

(b) What ranges were used

(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 required training sessions and specify reason for each delinquency.

(e) Names of all Bureau personnel who have failed to shoot qualifying scores with any authorized weapon. Include date last qualified.

(f) Any Bureau employee authorized to carry firearms who is delinquent, or fails to shoot qualifying scores after remedial training, automatically loses authority to carry firearms until the deficiency is dissolved.

(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.

(12) PFIs are to make every effort to ensure that the air quality of indoor ranges used by the field offices complies with the Occupational Safety and Health Administration (OSHA) standards. A copy of these standards is available upon request from the FTU. If an indoor range does not comply with OSHA standards, an effort should be made to locate an alternate facility.

(13)The authority in charge of a particular range should be advised of any safety deficiencies noted. Good judgment should dictate whether that facility can continue to be used until a deficiency is corrected.

EFFECTIVE: 05/20/94

12-10.1 Firearms Delinquencies

(1) Any SA authorized to carry firearms who does not attend firearms training during a firearms training period is considered delinquent. If a delinquency occurs, the employee must prepare a memorandum of explanation to the SAC documenting the circumstances for the absence. The SAC can either excuse the absence or rescind authority to carry firearms when an Agent becomes delinquent. No SA will be permitted to become delinquent for two consecutive firearms training periods. If this occurs, the SAC must require the employee to surrender his/her firearm unless the absence(s) is excused. The Firearms Training Unit (FTU) is to be advised of such instances 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.

(3) Delinquencies must be corrected as soon as possible.

(4) The identity of SAs who fail to attend firearms training sessions or meet minimum requirements during the calendar year must be listed in the annual report submitted to the FTU before 12/31 of each year.

(5) An unexcused delinquency from training is a serious matter and is not acceptable. If this deficiency persists, the SAC is required to inform the individual that the authority to carry firearms is rescinded. The weapon is to be surrendered and only reissued for training purposes. The individual is then unable to participate in raids or dangerous assignments which require the individual to be armed. FBIHQ must be advised of the delinquency and recommendations must be made to Administrative Summary Unit (ASU), FBIHQ, and FTU for appropriate administrative action.

EFFECTIVE: 05/20/94

12-10.2 Firearms Qualification

EFFECTIVE: 05/20/94

12-10.2.1 Firearms Qualification Policy

(1) All SAs must qualify with all weapons they are authorized to carry.

(2) All SAs must qualify four times per calendar year.

(3) SAs must qualify with each assigned handgun a minimum of once per year. It is recommended that the handgun regularly carried on duty be fired for qualification at each firearms session. The courses and scores fired annually are included in the Field Firearms Training Program for each calendar year.

(4) Specific training requirements are set out in the Field Firearms Training Program submitted by the Firearms Training Unit (FTU) for each calendar year. Principal Firearms Instructors are required to follow current established course protocols set by the FTU.

(5) Whenever authority to carry a weapon is rescinded, a memorandum of explanation should be attached to the SA's FD-40.

EFFECTIVE: 05/20/94

12-10.2.2 Recording 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. 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. FD-39s are retained for one year, then destroyed; FD-40 must accompany SA's personnel file

upon transfer.

(4) The scores of SAs on special assignments shall be furnished to their regular office of assignment.

(5) No SA shall calculate his/her own scores on record run courses.

EFFECTIVE: 05/20/94

12-10.2.3 Failure to Qualify

(1) If an SA fails to qualify, the Principal Firearms Instructor must provide remedial training and an opportunity to requalify on the next regularly scheduled qualification day.

(2) After opportunities have been provided for requalification and failures continue to exist, the Principal Firearms Instructor must advise the Firearms Training Unit by airtel 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, the SAC must require the employee to surrender his/her firearm.

EFFECTIVE: 05/20/94

12-10.2.4 Shoulder Weapons

SAs will qualify with each assigned shoulder weapon a minimum of twice per year. SAs with assigned weapons will use that specific weapon when qualifying.

EFFECTIVE: 05/20/94

12-10.3 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.

(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.

(d) Immediately upon picking up a firearm, face a safe direction, open the action and check to see that the weapon is unloaded. Check it again.

(e) Never give a firearm to or take a firearm from anyone, unless 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. Pay attention to instructors. You will be told exactly what to do.

(g) Perform safety check on the weapon before a training session. Make sure the weapon is unloaded before checking the barrel for obstructions. After training, you need only to make sure the weapon is unloaded.

(h) Load and unload only on the firing line and only as instructed. Any exceptions will be stipulated by the lead Firearms Instructor.

(i) Keep the firearm pointed down range or safe direction at all times.

(j) Use only one hand when holstering a handgun. Any exception will be so stipulated by lead Firearms Instructor.

(k) No smoking, eating or drinking on the firing line.

(l) No talking on the firing line except when instructed to do so.

(m) Never permit the muzzle of a firearm to touch the ground.

(n) In case of a misfire or malfunction, perform immediate action drill, unless instructed to do otherwise.

(o) 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.

(p) Never leave your firing position unless instructed to do so.

(q) Never remove a weapon from the holster in training, unless instructed to do so.

(r) Never dry fire on the range unless under direct supervision of a Firearms Instructor. Exceptions will be specifically identified by the lead Firearms Instructor.

(s) Eye and ear protection are mandatory when firing on the range. Ear plugs should be worn in conjunction with proper sound barriers.

(t) Everyone is responsible for range safety. Immediately report any safety violations you see to a Firearms Instructor.

EFFECTIVE: 05/20/94

12-10.4 Firearms Training of Noninvestigative 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 at the FBI Academy and FBIHQ.

(3) Other non-Agent personnel with special authority to carry firearms.

(4) All non-Agent personnel who are authorized to carry firearms will comply with all regulations in this section that normally refer to Agents. In addition, they must also attend annual legal training, quarterly defensive tactics training, and participate in the Fitness Indicator Test (FIT).

EFFECTIVE: 05/20/94

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.

(3) The Principal Firearms Instructor must ensure that ranges used for firearms training are inspected and contain no safety hazards that would endanger FBI or police personnel.

(4) Firearms demonstrations are to be given only by current firearms instructors.

EFFECTIVE: 05/20/94

12-10.6 Firearms Instructors

EFFECTIVE: 05/20/94

12-10.6.1 Policy

(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) RQC score 94

(c) PQC score 90

(d) Shotgun 10A score 90

(e) MP-5 (qualification course) score 94

(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 training session per year.

(4) Firearms instructors must attend a Recertification Program at the FBI Academy every 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: 05/20/94

12-10.7 Firearms Target Guidelines
Steel Target Policy

(1) For standard service and training ammunition, steel targets are not to be used at distances less than ten yards. Some types of frangible ammunition may allow use of steel targets at closer distances.

(2) To minimize ricochets, firing positions should be perpendicular to the target line.

(3) Steel targets must have a specific Brennel or American Rockwell rating to prevent "dimpling" of steel or complete penetration when impacted by bullets.

(4) Construction of any steel targets must be coordinated through the Firearms Training Unit.

(5) Principle Firearms Instructors are responsible for the use of proper weapons and ammunition on steel targets; i.e., use jacketed or frangible ammunition, no rifle ammunition used on steel designed only for pistol bullets, use of shotgun buckshot loads instead of rifled slug.

(6) Steel targets must be inspected before each training session.

(7) All personnel on the steel course site must stand behind the shooter. In multiple courses, the shooter must not be ahead of another shooter.

(8) All personnel on the steel course site must continuously wear eye and ear protection.

(9) Before use, Principal Firearms Instructors are to verify that the proper ammunition is used for each steel target system.

EFFECTIVE: 05/20/94

12-11 SHOOTING INCIDENTS (See MAOP, Part II, 8-1.3.2.)

EFFECTIVE: 05/20/94

12-11.1 Reporting of Shootings (See MAOP, Part II, 8-1.3.2.)

(1) In all shooting incidentr involving FBI personnel, notify FBIHQ by telephone.

(2) Incidents where Bureau personnel are present involving the discharge of a firearm 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 Congressional and Public Affairs, Attention: Correspondence Unit.

(4) SAC must personally ensure that investigations relative to Agent-involved shooting incidents are handled quickly and properly.

(5) SAC is to ensure that involved Agent(s) are removed quickly from the scene to reduce the effects of post-shooting trauma.

(6) Agents involved in a shooting must be given sufficient time to regain composure before giving any statements.

(7) Agent must understand his/her constitutional rights.

(8) Initial teletype should state whether an Inspector is required to conduct the inquiry.

(9) If an Inspector is not ordered to the scene, the SAC or ASAC must conduct an administrative inquiry when a weapon was discharged by FBI personnel.

(10) If the SAC or ASAC was involved in the planning or execution of events, FBIHQ should be advised during initial contact.

(11) The appropriate Assistant Director will advise Assistant Director, Inspection Division, relative to the need for an Inspector on the scene.

(12) If an Inspector is not dispatched to the scene, SAC will advise by teletype that he/she is conducting the necessary administrative inquiry, UACB.

(13)The SAC is responsible for preserving evidence and instituting a logical investigation.

(14)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/Inspector in consultation with FBIHQ officials. (See MAOP, Part I, 13-6 (3) and MIOG, Part I, 263-5 (3).)

(15)Results of administrative inquiry, in the form of an investigative report, are to be submitted to FBIHQ within two weeks.

(16)To assure accuracy and completeness, SAC should confer with the Chairperson, SIRG.

(17)Submit original and eight copies of report to Assistant Director, Criminal Investigative Division (CID), Attention: SIRG. CID will distribute to members of SIRG.

(18)The SIRG will provide to the Director evaluative analysis, observations, recommendations for corrective actions from an operational standpoint, and recommendations for administrative action.

(19)The SIRG is composed of representatives from:

(a) Criminal Investigative Division

(b) Inspection Division

(c) Personnel Division (PD)

(d) Training Division (TD)

(e) National Security Division

(f) Field supervisor (preferably one who has been involved in a shooting incident) from the Washington, D. C. area will serve as a permanent member of the SIRG.

(g) Office of General Counsel (nonvoting member; for legal analysis and advice to the SIRG).

(20)The report, which should have pertinent FD-302 interviews of participants and witnesses, signed, sworn statements of

principals involved, diagrams, and photographs, if appropriate, should be captioned "Administrative Inquiry, Shooting Incident, (name) Division, (date of shooting)" and should specifically reference, using the case caption, the teletype that initially advised FBIHQ of the shooting. Reference should also be made to the communication which forwarded the FD-418s.

(21) The SAC's recommendation(s) for any administrative action should be set forth on the administrative pages of the report.

(22) In joint 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:

(a) SAC or ASAC will notify FBIHQ by teletype.

(b) FD-418 must be submitted.

(c) Furnish promptly the complete results of investigation to include but limited to the following:

1. Activities of accompanying officer which led to the shooting.

2. Details of raid/arrest plan.

3. Instructions given to accompanying officer.

4. FD-302s of FBI witnesses and FBI personnel having knowledge of relevant events.

(d) FBI/controlled task force:

1. Include all of (c) above, plus:

a. Degree of FBI supervision exercised over the officer's day-to-day physical conduct.

b. Chain of command within the task force.

c. A copy of any Memorandum of Understanding on task force responsibilities.

d. A copy of the administrative inquiry report (if available) prepared by the local or state agency.

(e) Submit an original and eight copies of the

report to the Assistant Director, CID, Attention: SIRG, with one copy designated to the FTU.

EFFECTIVE: 05/20/94

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 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

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.

(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.

(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.

(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 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

12-11.6 Nondisclosure of Agents' Names in Shooting Incieents (See MAOP, Part II, 5-2 (3) 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: 05/20/94

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 Principal Firearms Instructor before use.

(4) Alterations to any holster are not permitted.

(5) Accessory equipment, i.e., magazine or speed loader pouches, ammunition pouches, handcuff pouches, etc., must be maintained and inspected in the same manner as 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 refer to shoulder holsters, belly bands, ankle holsters, inside pants holsters, cross-draw holsters, fanny (butt) packs.

(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: 05/20/94

| 12-13 [redacted]

b2
b7E

EFFECTIVE: 05/20/94

| 12-13.1 [redacted]

| (1) [redacted]

| (2) [redacted]

EFFECTIVE: 05/20/94

| 12-13.2 Description

| (1) [redacted]

| [redacted] (a) [redacted]

| (b) [redacted]

| (2) [redacted]

| (a) [redacted]

| (b) [redacted]

| [redacted]

4-750 (Rev. 12-14-88)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA DELETED PAGE INFORMATION SHEET

2 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 you or the subject of your request.

☐ Information pertained only to a third party. Your name 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 for the following reason(s): _____

☐ For your information: _____

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

MIOG, Part II, Section 12

XXXXXX
XXXXXX
XXXXXX

XXXXXXXXXXXXXXXXXXXXX
X DELETED PAGE(S) X
X NO DUPLICATION FEE X
X FOR THIS PAGE X
XXXXXXXXXXXXXXXXXXXXX

FBI/DOJ

1. [redacted]
2. [redacted]
3. [redacted]
4. [redacted]
5. [redacted]
6. [redacted]
7. [redacted]
8. [redacted]
9. [redacted]
10. [redacted]
11. [redacted]

b2
b7E

EFFECTIVE: 05/20/94

12-14 CHEMICAL AGENTS (See MIOG, Part II, 11-4.5.3.)

EFFECTIVE: 05/20/94

12-14.1 Policy

SAC approval is necessary prior to the use of chemical agent canisters, projectiles, aerosol grenades, or chemical smoke.

EFFECTIVE: 05/20/94

12-14.2 Procedure

(1) SAC approval is not necessary before using chemical agent aerosol Individual Protective Device (IPD).

(2) Whenever chemical agents are deployed in any form, advise FBIHQ and the Firearms Training Unit (FTU) by airtel with FD-418 attached outlining use and detailed results within five working days of the incident.

(3) Whenever an IPD is used, an FD-418 must be executed within five working days and submitted to the FTU.

(4) Only SAs who have received proper training are authorized to use weapons delivery and hand deployed chemical agent systems, including IPDs.

(5) SAs or other authorized employees are prohibited from transporting any chemical agent material in the passenger compartment of commercial aircraft.

(6) [redacted] b2 b7E

(7) Only chemical agents and IPDs approved by the Training Division are permitted for official use.

(8) Use, Effects and Maintenance

(a) The chemical agents used by the Bureau are:

1. [redacted]
2. [redacted] b2 b7E

(b) Gas masks should be available for all Bureau personnel exposed to chemical agents.

(c) Chemical agents should always be deployed "down wind."

(d) Where possible, deploy chemical agents at a level lower than the location of Bureau personnel because the chemicals are heavier than air.

(e) During short-term exposure, chemical agents will not damage the lungs.

(f) Under long-term exposure, chemical agents can be lethal.

(g) Chemical agents displace oxygen and in confined areas, can cause asphyxiation.

(h) [redacted] b2 b7E

(i) Chemical agents produce severe eye irritation, tearing and skin inflammation and stinging.

(j) Irritation should disappear by washing with soap and cold water and exposure to fresh air.

(k) Do not rub eyes as this may promote additional irritation.

(l) Do not bandage eyes.

(m) Replace clothing exposed to chemical agents as they retain the contaminants for long periods of time.

(n) Seek medical attention after exposure to chemical agents, if eye inflammation or skin rash persists.

(o) When a person is sprayed with an IPD, do not leave that person unattended. Keep the individual in an upright position until the effects of the chemical wear off. Proper aftercare procedures must be administered.

(p) Chemical agent projectiles are considered lethal when fired at a person.

(q) Chemical agents should be stored in a cool dry place.

(r) After expiration date, chemical agents should be replaced.

(s) Expired chemical agents may be used for training.

(t) When an IPD is first issued, depress activation button for one-half second test spray to ensure device is working properly. This must be done outdoors in the absence of people.

EFFECTIVE: 05/20/94

12-14.3 Hand-Thrown Chemical Agents

(1) Deployment of chemical agent grenade

(a) Hold grenade with detonator strap in palm of the throwing hand.

(b) Do not hold detonator strap with fingers.

(c) Safety ring should always face inward so thrower does not have to reach across the grenade for removal.

(d) Remove pin and retain until grenade detonates.

(e) If deactivation becomes necessary, pin can be replaced.

[redacted] (2) [redacted] b2 b7E

(3) [redacted]

(4) [redacted]

EFFECTIVE: 05/20/94

12-14.4 Chemical Agent Delivery Systems and Projectiles

(1) [redacted]

	Maximum Range	Estimated Effective Range
(a) [redacted]	[redacted]	[redacted]

b2 b7E

4-750 (Rev. 12-14-88)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA DELETED PAGE INFORMATION SHEET

2 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 you or the subject of your request.

☐ Information pertained only to a third party. Your name 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 for the following reason(s): _____

☐ For your information: _____

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

MIOG, Part II, Section 12

XXXXXX
XXXXXX
XXXXXX

XXXXXXXXXXXXXXXXXXXXXX
X DELETED PAGE(S) X
X NO DUPLICATION FEE X
X FOR THIS PAGE X
XXXXXXXXXXXXXXXXXXXXXX

FBI/DO

[redacted]

b2
b7E

(2) [redacted]

(3) [redacted]

(4) [redacted]

(5) [redacted]

(a) [redacted]

(b) [redacted]

(6) [redacted]

(7) [redacted]

(8) [redacted]

(9) Repair parts for Bureau masks are available through the Firearms Training Unit.

(10) Protective masks should be cleaned with a damp cloth after having been contaminated.

EFFECTIVE: 05/20/94

12-14.8 Cleaning (See MIOG, Part II, 11-4.5.3.)

b2
b7E

[redacted] should be cleaned with soap and boiling water to remove residue. Thoroughly dry all metal parts and lubricate with light coat of oil.

EFFECTIVE: 05/20/94

12-15 DEMONSTRATIONS AND TOURS

(1) Only authorized firearms instructors will present "live fire" weapons demonstrations.

(2) Any other SA may present Bureau firearms for demonstration using "red-handle" weaponry or properly deactivated live weapons equipped with trigger guard locks or other similar device which prevents the weapon from firing.

(3) The safe condition of all weapons used for demonstration should be employed whenever possible. (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: 05/20/94

12-16 MEDICAL PROFILE SYSTEM - MEDICAL MANDATES (RESTRICTIONS)

(1) When a physician assigns medical mandates (restrictions), advise Fitness-for-Duty Subunit (FFD), Health Care Programs Unit (HCPU), FBIHQ (UACB) such action has been taken. Ensure employee submits the requested medical statements supporting his/her current medical/physical status from his/her personal physician as requested by FFD, HCPU.

(2) The SAC or division head is instructed to contact the Performance, Recognition and Awards Unit (PRAU), for guidance regarding the employee's duties and responsibilities. This will ensure that any modifications necessary to the employee's Performance Plan will reflect the employee's assigned duties and will assist in preparing his/her Performance Appraisal Reports.

(3) Agents on medical mandates are to be permitted to participate in firearms training, exclusive of defensive tactics, provided the Agent's evaluating physician is fully familiar with the Agent's condition and is aware of the nature of the firearms 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).)

(4) In those instances where the evaluating physician does not certify the Agent to attend firearms training and the

prospects for future firearms participation are remote due to the Agent's condition, authority to carry a firearm is to be denied and any Bureau-issued weapon turned in. (See MAOP, Part I, 20-5.2.1 (3).)

EFFECTIVE: 05/20/94